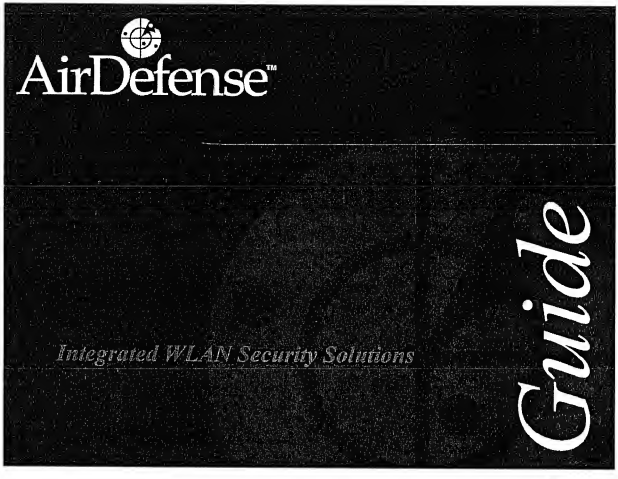
EXHIBIT A


AirDefense™
Integrated WLAN Security Solutions
User Guide
Release 3.0

AirDefense User Guide
Issue 1.02, AD-UG-1.02, Release 3.0
[redacted]

Proprietary Notices

AirDefense is licensed software and hardware. Its use is subject to the terms and conditions of a license agreement or nondisclosure agreement between AirDefense, Inc. and its customers. It is against the law to copy the software on any medium except as specifically allowed in the license or nondisclosure agreement.

Information contained in this document is subject to change. No part of this manual and/or software may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than personal use by AirDefense, Inc. without the express written permission of AirDefense, Inc.

Trademarks

AirDefense™ is a trademark of AirDefense, Inc. in the U.S. and other countries.
All other trademarks are the property of their respective owners.

Cautionary Statements

- **Caution:** There are no user-serviceable components inside the AirDefense Server appliance. Opening the chassis will void your service agreement.
- **Caution:** The recommended ambient operating temperature of the AirDefense Server appliance is 0°C—55°C. Installation in a closed or multi-rack assembly may raise the immediate ambient temperature above the average room temperature. Exercise due caution.
- **Caution:** Provide adequate spacing above, below, and behind the AirDefense Server appliance, to allow proper air flow, and to prevent excessive heat buildup.
- **Caution:** Use only industry-standard mounting kits when installing the AirDefense Server appliance, as improper mounting may result in hardware failure and hazardous conditions.
- **Caution:** Ensure that the electrical circuit through which the appliance is powered can safely accommodate the AirDefense Server's 300 Watt power supply.

Publication History

[redacted]

Issue 1.00 of this document, for AirDefense software Release 2.0

Issue 1.01 of this document, for AirDefense software Release 2.1

Issue 1.02 of this document, for AirDefense software Release 3.0

Contents

i Introduction

Welcome to AirDefense-the key to providing your wireless local area network (WLAN) with the most advanced security solution available today.

This Introduction contains the following topics.

i.1 About this Guide

This guide describes how to install, operate, and administer the AirDefense™ wireless network protection and management system. This guide includes the following major topics:

- What is AirDefense?
- Installation and Logging On
- Operation
- Administration

Useful Tips

You will find useful tips from AirDefense, Inc. in blue boxes throughout this guide.

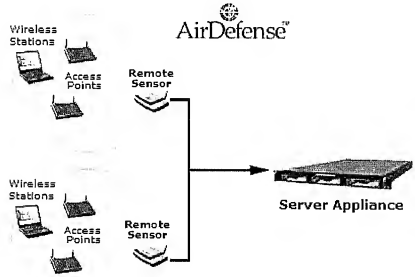
i.1.1 Audience

The audience for this guide includes AirDefense customers and partners who wish to deploy the AirDefense wireless LAN protection and management system in their WLAN. Familiarity with wireless networks is advisable.

AirDefense is a WLAN intrusion protection and management system. It consists of three components: physical Sensors that are placed at strategic locations in your WLAN; a management appliance--the AirDefense Server--that receives information from the Sensors; and a management console that runs the AirDefense Server.AirDefense authorizes and monitors the traffic of every User Station (wireless-capable laptops and workstations) in your WLAN.

AirDefense does the following:

- Provides proactive WLAN defenses. AirDefense discovers network vulnerabilities and threats – such as rogue Access Points and ad hoc networks – as they happen.
- Detects intruders and attacks on the WLAN, and eliminates those threats.
- Provides robust WLAN management functions that allow you to understand your WLAN, monitor network performance, and enforce network policies.



i.2.1 The AirDefense Solution

The AirDefense solution consists of distributed Sensors and centrally managed Servers that reside near 802.11 Access Points.

- The AirDefense Server analyzes traffic in real time to detect intrusions, impending threats, and attacks.
- Sensors monitor all WLAN activities and report back to the AirDefense Server, which analyzes the traffic in real time.The Sensors provide 24x7 monitoring of WLAN traffic and activities. Sensors are centrally managed by the AirDefense Server.

With its combination of properly deployed Servers and Sensors, AirDefense enforces WLAN policies, monitors WLAN performance, helps network administrators troubleshoot network issues, and provides comprehensive reporting. AirDefense is configurable, so you can identify both authorized and unauthorized Stations and Access Points that are transmitting and receiving data within your network— even users on the perimeter of your wireless air space.

AirDefense is the only WLAN security solution that provides 24x7, real-time tracking of the airwaves. It monitors the state of every Access Point and Station transmitting on the airwaves and gives you a minute-by-minute account of all WLAN hardware statuses and wireless traffic.This enables you to immediately recognize intruders, quickly detect attacks, and take appropriate measures to secure the network. A patent-pending State-Analysis Engine enables AirDefense to track and control the flow of communication on any enterprise WLAN.

Multi-Dimensional Detection and State Analysis Engines

AirDefense built its patent-pending Multi-Dimensional Detection Engine as a WLAN intrusion detection system.

A traditional intrusion detection system (IDS) is plagued by false positives because they rely on a single detection technology—mostly attack signatures. AirDefense has developed its Multi-Dimensional Detection Engine as a comprehensive WLAN intrusion detection system that integrates multiple detection technologies. These technologies correlate data to recognize real threats and reduce false positives. The State-Analysis Engine coordinates inputs and the Multi-Dimensional Detection Engine analyzes threats to identify security breaches based on:

- Signature analysis
- Policy compliance
- Protocol assessment
- Statistically anomalous behavior

AirDefense consists of a AirDefense Server and one or more Sensors. The AirDefense Server has two user interfaces; the Sensor has one user interface.

- AirDefense Server
  - — AirDefense Command Line Interface
  - — AirDefense Graphical User Interface (GUI)
- Sensor
  - — Sensor User Interface (UI)

i.3.1 AirDefense Command Line Interface

The AirDefense Command Line Interface is the interface you use to do the initial local setup of the AirDefense Server. After the initial setup, you only use the Command Line Interface to perform specific configurations that are not available using the AirDefense Graphical User Interface (GUI). For example, you must use this interface to update the AirDefense Server's network settings.You will find detailed information regarding the Command Line Interface in Chapter 9, Command Line Interface.

You can access the Command Line Interface directly from the AirDefense Server via attached keyboard and mouse or via an SSH connection.

i.3.2 AirDefense Graphical User Interface (GUI)

The AirDefense GUI is the interface where you do most of the daily and operational and administrative tasks in AirDefense.

The GUI interface is assessable by logging on remotely from a secure web browser. It is not accessible from the AirDefense Server.

Navigation Buttons on the AirDefense GUI

At the top of every page are seven named icons that represent each of AirDefense's program areas. Clicking once on an Icon takes you directly to the program area.

The table below lists the program areas in the GUI.

Program	This Program Enables You To...
Dashboard	• View a cumulative daily overview of AirDefense detection results--a brief overview of your wireless network. The tables in Dashboard display a summary of authorized and unauthorized Access Points and Stations, the devices responsible for generating the most recent alarms, the devices that most recently violated wireless network policies, and an overview of Sensor channel. • Filter the most recent alarm data that displays for each individual Sensor, or Sensors within a Group or Location. *Note:* A ***device*** is a Sensor, Access Point, or Station. How a device is represented in the GUI is influenced by user preference settings. *Note:* Channel activity displays for one Sensor at a time. AirDefense defaults to the first Sensor in an alphanumeric list of Sensors in your WLAN.
Alarms	• View detailed, real-time information about the alarms that AirDefense generates when one of its Sensors detects network traffic indicative of a network attack, intrusion, or policy violation, including when the alarm was generated, what condition triggered the alarm, and the devices associated with the alarm. • Filter which alarms can generate, to group the alarms into priorities, and to determine when you are notified of an alarm.
Sensor	• Configure settings for each Sensor and groups of Sensors deployed—their network settings and operating modes. • See a Sensor in your WLAN.
Policy	• Create and apply policies for your Access Points (such as which Stations may associate with them, and whether WEP is required, etc.) • Set performance thresholds used to generate alarms for abnormal traffic patterns • Specify hours in which wireless network traffic is allowed. • Add Access Points and Stations to your network, either manually or by import. • Monitor the historical associations and behaviors of the devices in your network.
Notification	• Specify how AirDefense delivers alarms and reports.Your choices are: — Alarm Notification — Daily Security Report — Daily Network Report — Daily and Weekly Management Report • Notification also allows you to choose the delivery method: email or SNMP traps.

Program	This Program Enables You To...
Reports	• View summaries and detailed information about your Sensors, Access Points, Stations, and AirDefense Performance. Reported, for example, are how many bytes of data each Access Point has transmitted, a breakdown of Control, Management, Data, and Error frames, high, low, and mean signal strength between Access Points and Stations. • Print the Reports.
Admin	• Provide AirDefense with user names, roles, and password information • Configure your display preferences • Export and backup AirDefense data • Update the AirDefense software • Request and install security certificates • Name your AirDefense system.

Status Indicator

Located at the top-right of each page are two status lights—one **green**, and one **red**. These lights indicate AirDefense's current status. AirDefense monitors its own system status. If components do not function as designed, AirDefense restarts the component.

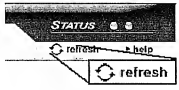
- A green light indicates that the AirDefense Server is operating as designed—all systems are functioning normally.
- A red light indicates that one or more components of AirDefense are not operating as designed, or that a restarted component has failed more than once in a 24-hour period.

Important–AirDefense Technical Support

If a red light displays on the AirDefense Server, contact AirDefense Technical Support for assistance at **770-663-8115**, or by email at **support@airdefense.net**

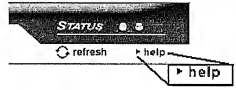
Refresh

Except for the Dashboard, which updates its display every minute, AirDefense's windows are static. The data is accurate as of the minute you open a page or load a report. A **Refresh** button at the top right of the window enables you to query AirDefense's database for new, updated information and display it on screen.



Help

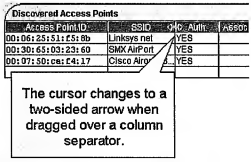
Beneath the Status Indicator is a Help button that offers options to open an About dialog that provides application version information, or open online, context-sensitive help.



Tables

AirDefense displays much of its data in a tables. You may re-size the width of table columns by dragging the column separators with your mouse. (Column size persists as pages are refreshed, but not if the screen reloads. In this case, the columns return to their default size.)

You may sort the contents of the table by clicking any column heading.



1.3.3 Sensor User Interface (UI)

The Sensor User Interface (Sensor UI) is an HTML-based interface that you use to initially configure Sensor network settings and select a Sensor's mode of operation. Each Sensor contains a small web server that administrators can use to access the Sensor via their favorite browser.

Typically, you configure Sensors once, using the Sensor UI. In some cases (see the note that follows), you can use the AirDefense GUI to perform some maintenance on Sensors (see Chapter 4, Sensor Manager). Additional administrative trips to the Sensor UI are only needed if your wireless network architecture changes, for example, if you add Sensors to your network.

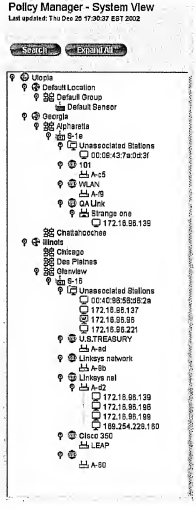
> ***Note:*** The web-based Sensor UI is nearly identical to the interface for Sensor configuration in the AirDefense GUI. There are two selections that you can only make from the Sensor UI: the Currently Online toggle and the Sensor's Security settings. For more information on how to configure the Sensor using the Sensor UI, see "Configuring Sensors" on page 19.

Color-coded icons display throughout the AirDefense GUI. These icons represent the presence and associations of Sensors, Access Points, and Stations in your network, and their states.

- Icons identify network elements and their associations in the network.
- Colors identify the state of each network element.

i.4.1 Tree View

You will find color-coded icons in the Tree View of many GUI programs.The illustration below shows a typical Tree View screen.



Tree View is a true, structured hierarchy, with the highest level at AirDefense (system) View and the lowest level at Station View. The tree uses color-coded icons to show the Location, Group, Sensor, Access Point, and Station associations in your WLAN network. In GUI programs where the Tree View appears, you can click on the **individual** network elements in the tree to access their configuration screens.

> ***Note:*** Locations, Groups, Sensors, and Access Points appear only in one place on Tree View. Stations can appear in more than one place on Tree View, matching their associations with Access Points.

i.4.2 Color Codes

Each icon in Tree View has a color that represents a state.

- Individual Access Points and Sensors display in a single color that represents their current state.
- A single Station can display in two or more colors, depending on its configuration in relationship to its Access Point.

> ***Important:*** In certain cases, the meanings of icons may differ slightly, depending on if the icon appears in the Tree View, or on one of the many screen tables that appear throughout the GUI.

The table on the next page lists the colors and their meanings.

Color	Meaning
Blue	Blue indicates a default placeholder state for Sensors, Access Points, or Stations that are not observed by AirDefense. Placeholder items are always a manually-added or an imported Access Point or Station. ***They will always be Blue.*** ***Note:*** When you import an Access Point that has never been entered into AirDefense, it will be Blue, even if you authorized in its configuration in the import file. When AirDefense detects the newly imported Access Point, the state changes to either authorized (Green) or unauthorized (Red), depending on your configuration in the import file.
Grey	Grey indicates that a Access Point or Station is being ignored by the AirDefense Server. For more information on Ignore, see Chapter 5, Policy Manager. ***Note:*** AirDefense sees devices that are in the ignored state, but does not generate an alarm unless an attack occurs.
Red	Red indicates the following: • **Sensor:** Offline, which indicates that the Sensor is not communicating with the AirDefense Server for one of the following reasons: — Sensor has been observed by the Server, but is currently not connected to the Server. — Sensor is connected to the Server, but is configured for **Active: no** operation (see "Configuring Sensors" on page 19). ***Note:*** If you did not intentionally take a Sensor offline, perform appropriate steps to reboot the Sensor (see Chapter 1, Installation & Log In). • **Access Point:** Unauthorized — All Access Points are unauthorized when they are first discovered by AirDefense. They remain unauthorized until an administrator changes their state to authorized. If you manually add or import an Access Point, you can configure it as authorized at that time, in which case, it enters AirDefense as Blue. • **Station:** Unauthorized on a given Access Point — Unauthorized indicates that the Station is not authorized for the Access Point it appears under — The same Station can appear as Red or Green, depending on whether or not they are authorized on the Access Point they are under — Stations have a W on Green or Red if they are on the user-configurable Watch List (for more information on the Watch List, see Chapter 5, Policy Manager). ***Note:*** AirDefense generates an alarm once per minute, per device, as long as the device remains unauthorized.

Color	Meaning
Green	• Stations — Station is authorized under the Access Point and has been observed as associated to that Access Point • Access Points — Access Point is authorized and has been observed by a Sensor • Sensor — Green indicates that the Sensor is functioning normally and in communication with the AirDefense Server.To be in this state, the following is required: >>The Sensor must be connected to the Server--the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). >>The Sensor must be configured for **Active: yes** operation (see "Configuring Sensors" on page 19).
Purple	Purple can have two meanings: • In all GUI program areas with the exception of Policy Manager, Purple indicates that the Station has been observed, but not currently associated, with any Access Point at that time. • In Policy Manager, Purple indicates that a Station has never been associated with an Access Point.
Orange	Orange indicates Ad Hoc activity. There are two Orange icons: • Ad hoc Network • Ad hoc Station

1.4.3 Icons

Each network element in the AirDefense WLAN is represented by an icon. Icons can either represent a physical device, such as an Access Point, Station, or Sensor, or logical associations, such as an SSID, a Location, or a Group.

The tables below list the icons and their meanings:

Magnifying Glass

Icon	Color/State	Meaning
	Static	Magnifying Glass. This icon can appear on all items in the Tree View with the exception of the Station. It indicates that the item is expandable or collapsible. Clicking on the icon next to a tree item expands that item; clicking again, collapses the item. For example, clicking on the magnifying glass next to an Access Point reveals the Stations that have associated with that Access Point.

AirDefense (System) Icon

Icon	Color/State	Meaning
	Static	This is the highest level in the tree, representing the AirDefense Server.

Location Icon

Icon	Color/State	Meaning
	Static	This is the second highest level in the tree, representing the Sensor Location. Expand the Locations to expose the individual Groups for a particular Location.

Group Icon

Icon	Color/State	Meaning
	Static	This is the third highest level in the tree, representing the Sensor Group. Expand the Groups to expose the individual Sensors for a particular Group.

Sensor Icons

Sensors can be three different colors, representing three states. These are Blue, Red, and Green. Sensor icons can also have a CH or SC on the icon. The CH indicates that the Sensor is configured for Channel Lock; the SC indicates that the Sensor is configured for Scan Channels (see "Configuring Sensors" on page 70 for more information on these configurations). .

Icon	Color/State	Meaning
	Blue: Not observed by the AirDefense Server; not online or active	Default Sensor The Default Sensor is a placeholder, not a real online Sensor. This is a place to put Stations and Access Points that you have manually added or imported, and authorized into AirDefense. AirDefense has not yet physically observed these. ***Note:*** Access Points entered into AirDefense always appear as blue, and always at the top of the tree under Default Sensor until they are seen by AirDefense. Once observed, they become green, red, or grey, and are moved out of the list, but not automatically. You must click **Refresh**.
	Green: Online **CH**=Channel Lock **SC**=Channel Scan	Online Sensor Sensor is functioning normally and is communicating with the AirDefense Server.To be in this state, the following are required: • The Sensor must be connected to the Server--the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). • The Sensor must be configured for **Active: yes** operation (see "Configuring Sensors" on page 19).
	Red: Offline **CH**=Channel Lock **SC**=Channel Scan	Offline Sensor Sensor is not communicating with the AirDefense Server for one of the following reasons: • Sensor has been observed by the Server, but is currently not connected to the Server. • Sensor is connected to the Server, but is configured for **Active: no** operation (see "Configuring Sensors" on page 19).

SSID Icon

Icon	Color/State	Meaning
	Static	SSID This is the logical group to which the Access Points belong.

Access Point Icons

Access Points and Bridged Access Points can be four different colors, representing four states. These are Blue, Red, Green, and Grey.

Icon	Color/State	Meaning
	Blue: Unobserved	Unobserved Access Point Access Points that are blue are not yet seen by a Sensor.
	Blue: Added Access Point Folder	Added Access Point Folder This folder contains Access Points that have been added manually or imported, but have not yet been seen by a Sensor.
	Green: Authorized	Authorized Access Point ***Note:*** Access Points that you enter manually or import are appear as blue, and always at the top of the tree under Default Sensor. Once they are seen by AirDefense, they are moved out of the list, but not automatically. You must click **Refresh**.
	Red: Unauthorized	Unauthorized Access Point On discovery, all Access Points come into AirDefense unauthorized. ***Note:*** An exception to this is if you previously added or imported the Access Point, at which time you can choose to authorize the Access Point. When it is seen by AirDefense, the Access Point will change from blue to green and move under the discovering Sensor.
	Grey: Ignored	Ignored Access Point Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates alarms. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.
    	Blue: Unobserved Green: Authorized Red: Unauthorized Grey: Ignored	Bridged Access Point ***Note:*** Bridges are user-defined for informational purposes. Two or more Access Points can serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired Access Point. For more information, see Appendix D on page 259.

Station Icons

Stations can be five different colors, representing five states. These are Purple, Green, Red, Grey, and Orange.

- Green and Red Stations can have a "W" on the icon, indicating they are on the Watch List.
- A Stations can appear as Green, Red, or Grey under different Access Points, depending on the configuration.

Icon	Color/State	Meaning
	Purple: Unassociated Purple with "W": Authorized, and on Watch List	Unassociated Station Purple Stations have two meanings: • In all GUI program areas with the exception of Policy Manager, a Purple Station indicates that the Station has been observed, but not currently associated with any Access Point at that time. • In Policy Manager, a Purple Station indicates that the Station has never been associated with an Access Point. It always appears under the Unassociated Stations folder in Policy Manager.
	Green: Authorized Green with W: Authorized, and on Watch List	Authorized Station This is a Station that is authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List. ***Note:*** An authorized Station may appear as Unauthorized (Red) or Ignored (Grey) under a different Access Point.
	Red: Unauthorized. Red with W: Unauthorized, and on Watch List	Unauthorized Station This is a Station that is not authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List. Unauthorized Stations generate alarms once per minute, per MAC address, for as long as the AirDefense Server recognizes the Station. ***Note:*** An unauthorized Station may appear as Authorized (Green) or Ignored (Grey) under a different Access Point.
	Grey: Ignored	There are two types of Grey Stations: • Station is configured for Ignore--*not alarm generating* — All activity by this Station is ignored by AirDefense. It does not generate alarms in AirDefense, regardless of activity. • Access Point is configured for Ignore--*alarm generating*. — If you configure an Access Point as Ignored, any Station under the Access Point also become Ignored in terms of traffic on that Access Point. If the Station starts doing anything outside of configured policies, AirDefense generates alarms.

Icon	Color/State	Meaning
	Orange: Ad Hoc:	Ad Hoc Station An ad hoc Station is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc Stations and reports the network's Device Identifiers and other information.
	Grey folder/Blue Station: Unassociated	Unassociated Stations The Unassociated Station folder contains Stations in a manual state that are observed by the AirDefense, but that have never been associated with an Access Point. Stations under this folder appear as Purple.

Ad Hoc Network Icon

Icon	Color/State	Meaning
	Orange: Ad Hoc	Ad Hoc Network An ad hoc network is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc networks and reports the network's Device Identifiers and other information. ***Note:*** The software that controls the functionality of wireless network adapters typically provides the ability, configured manually, to accomplish ad hoc networking.The software creates a session ID—much like the MAC address of an Access Point—which the devices use to communicate with each other.

Device identifiers for each Access Point, Station, and Sensor display throughout the AirDefense GUI.

Example: *Access Points can display throughout the GUI as either a MAC address, an IP address, a Name you select, or as a DNS name.*

You can determine which type of identifier you want to display for each device type.To do this you must use the AirDefense GUI to access **Administration>User Preferences** and make a display selection for each device type. Your selections in this program area determine which Device Identifier a device has in all GUI screens. For complete information on how to use this feature, see "User Preferences" on page 221.

Note: The AirDefense default is to display IEEE MAC address for each device.

The table below lists the display preferences for device identifiers...

Device	Preference (You can choose one)
Access Points	• MAC address • IP Address • Name • DNS (name)
Stations	• MAC address • IP Address • Name • DNS (name) • LEAP (name)
Sensors	• MAC address • IP Address • Name

AirDefense listens to wireless network traffic, in real time, 24x7. It uses **three** different lengths of time in its reporting: These are:

- Minute
- 24 hours
- 30 days

i.6.1 Minute

AirDefense reports statistics every minute. For example, the AP Statistics Report shows a variety of network traffic statistics for each Access Point on a minute-by-minute basis.

i.6.2 24 Hours

AirDefense maintains cumulative data over a 24-hour period beginning each day at midnight. What displays in AirDefense's Dashboard, for example, is information about your WLAN activity that has accumulated since midnight.

i.6.3 30 Days

AirDefense keeps most data (e.g., traffic statistics) in its database for 30 days, after which, it deletes it. Many of the Reports, for example, will display data for the previous 30 days. (You may export AirDefense's data for archival purposes at Administration > Data Export—see Chapter 8, Administration).

1 Installation & Log In

AirDefense components consist of an AirDefense Server and one or more Sensors.

- The AirDefense Server is designed to be rack-mounted with your other network appliances.
- Sensors are small and lightweight enough to be placed in almost any location--a cabinet, or on top of a cubicle or bookshelf.

1.0.1 In This Chapter

This chapter contains the following topics.

1.1 Installing the AirDefense Server

Physical installation of the AirDefense Server consists of installing the device into a 19-inch rack and providing power and network connectivity. A keyboard, mouse, and monitor may be attached, allowing a direct connection. Alternately, administrators can access the appliance remotely, via web browser or SSH client.

Important: Please read all cautionary statements at the front of this guide before installing this product.

1.1.1 AirDefense Server Physical Installation Steps

Follow the steps below to physically install the AirDefense Server.

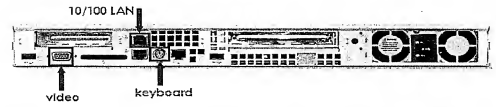
Steps to Physically Install the AirDefense Server

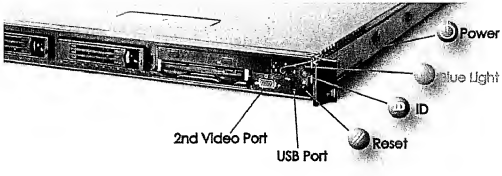
Step	Action
1	Install the AirDefense Server into a standard EIA 19-inch rack. Tighten the mounting screws (there is one on each side of the faceplate).
2	Attach power, monitor, mouse, and keyboard cables.

3 Connect the AirDefense Server to the network.

Connect the Ethernet cable to the top 10/100 LAN port on the back panel.

See the illustrations that follow.





Your network administrator must assign an IP address, subnet mask, and host name for the AirDefense Server. The AirDefense Server ships with a default DHCP.

To change the default settings, you must attach a keyboard, mouse, and monitor to the AirDefense Server and log on to AirDefense's Command Line Interface. Use this interface to change the settings.

1.2.1 Connecting the AirDefense Server to the Network

Follow the steps below to connect the AirDefense Server to the Network.

Steps to Connect the AirDefense Server to the Network

Step	Action
1	Turn on power to the AirDefense Server. *As the AirDefense Server is booting up, a command-line log on prompt will appear.*
2	Enter the following: *User Name:* ***smxmgr*** *Password:* ***(supplied in your shipping materials)***
3	Enter **ADDadmin.** *The ADDadmin terminal window opens.*
4	Type **n** at the command prompt. *This opens the network settings screen.*
5	Type **ip.** *This opens the network screen, which displays the current network configuration in bold text. Use this screen to change the IP address, subnet mask, and default gateway for the AirDefense Server.*
6	At the prompt, enter the new IP address and press **Enter.** *You are prompted to enter a new subnet mask.*
7	Enter the new subnet mask and press **Enter.** *You are prompted to enter the new gateway.*
8	Enter the new gateway address and press Enter. *Your new values display in bold text.*
9	Check the values **carefully** for accuracy.
10	Type **Yes** or **No** to commit the changes. *If you commit incorrect information, you will not be able to access the AirDefense Server over the network.* *Once you type* **Yes** *or* **No**, *you will return to the previous Network Screen.*

11 From the Network screen, configure the remaining network settings. For each property page, type the following at the command prompt and provide the required information for each property. For an explanation of the settings, see the table below.

***dns** for the DNS AirDefense Server*

***hname** for the Host name*

***dname** for the Domain name*

***mrelay** for the Mail Relay*

***arp** for the ARP table*

***hallow** for Allowed Hosts*

***hdeny** for Denied Hosts*

***ping** for enable/disable AirDefense Server ping*

Network Setting	Meaning
dns	Domain Name Server. This is the name of the AirDefense Server you give your DNS server. Your DNS server will match the name of the AirDefense Server with its IP address.
hname	Host Name. This is the name assigned to the computer that acts as a server for other computers on the network. For instance, a web host is what provides the content of web pages to the computers that access it.
dname	Domain Name. This is the name that identifies a web site. For example, "apple.com" is the domain name of Apple Computer's web site. A single web server may have more than one domain name, but a single domain name points to only one machine.
mrelay	
arp	Address Resolution Protocol. ARP is a TCP/IP protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. ARP returns the layer 2 address for a layer 3 address. ARP requests are broadcast onto the network, requiring every station in the subnet to process the request.
hallow	
hdeny	
ping	The main purpose of a ping is to test a system on the Internet to see if it is working. "Pinging" an AirDefense Server can test the response time of the Server while connected to the Internet. This is helpful in finding Internet bottlenecks, so that data transfer paths can be re-routed the most efficient way.

12 Type **Yes** to save the input to each screen

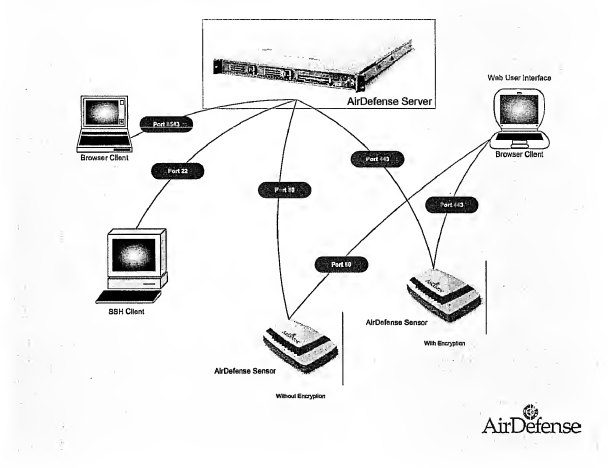
13 Type **q** to return to the ADDadmin main menu.

14 Type **q** again to quit the application.

The system automatically reboots.

Connection Confirmation

The illustration and table that follow shows all ports that must be open for communication between the AirDefense Server and its Sensors, and for administrative sessions with the AirDefense Server.



Port	Connection Between...
8543	Browser client and AirDefense Server
22	SSH client (only) and AirDefense Server
80	• Sensor and AirDefense Server--No Encryption • Sensor and Web User Interface Browser Client--No Encryption
443 (https-Secure)	• Sensor and AirDefense Server--Encryption • Sensor and Web User Interface Browser Client--Encryption

AirDefense requires a valid logon to access the AirDefense GUI or the Command Line Interface. You may access these interfaces either locally (console) or remotely (web).

1.3.1 Local Logon--Console

Follow the steps below to configure settings for a local AirDefense Server.

- You must use the Command Line Interface to log on to a local AirDefense Server.
- You must have a console--monitor, keyboard, and mouse--attached to the AirDefense Server.

Note: AirDefense provides a command-line utility called **ADDadmin** (AirDefense Device Admin) that allows you to configure settings for the AirDefense Server. Some of these settings are not possible using the AirDefense GUI.

Steps to Power Up and Log on to a Local AirDefense Server using the Command Line Interface

Step	Action
1	Turn on power to the AirDefense Server. *As the AirDefense Server is starting up, a command-line logon prompt appears.*
2	At the logon prompt, enter the user name **smxmgr** and the unique password for your organization. *This connects you to the AirDefense Server.*
3	Enter the command **ADDadmin**--*the command is case-sensitive.* *This launches the Command Line Interface* *The ADDadmin screen appears*

1.3.2 Remote Logon--Web

There are prerequisites for a remote logon. You must have the following:

- Either a web browser or SSH client application at the workstation
- Java® Runtime Environment® on your workstation
- SSL 3.0 selected in your Microsoft® Internet Explorer® options.

Web Browser or SSH Client

You must have either a web browser (http through Port 8543) or SSH client application (through Port 22) at the workstation

Java Runtime Environment

Confirm that you have Java Runtime Environment (JRE) 1.4.0 or 1.4.1on your workstation. The most widely-used browsers—Internet Explorer, Netscape®, Mozilla®—do not include the Java Runtime Environment as a default. If you do not have it on your workstation, you must manually install the JRE plug-in. The plug-in is free from Sun Microsystems®. The download page is: **http://java.sun.com/j2se/1.4/download.html.**

Do the following to check your current version of JRE.

Step	Action
1	Bring up you system command prompt (C:\). *To do this, use the following path from your Windows Start menu:* ***Start>Programs>Accessories> Command Prompt.***
2	Type in the following at the command prompt: **java -version**. Click **Enter.** *(There is a space between java and the hyphen.)*

SSL 3.0

Confirm that you have selected SSL 3.0 in your Microsoft Internet Explorer internet options. To confirm this, do the following:

Step	Action
1	Bring up you system command prompt (C:\) *To do this, use the following path from your Windows Start menu:* ***Start>Settings>Control Panel> Internet Options.*** *The Internet Properties screen appears.*
2	Click on the **Advanced** tab of the Internet Properties screen.
3	Scroll down the screen until you find the checkbox **Use SSL 3.0.**
4	Make certain the box is checked.

You can log on to AirDefense's GUI or Command Line Interface from a remote workstation.

Note: The AirDefense Server must already be powered up and running.

Steps to Log On to a Remote AirDefense Server using the GUI

Step	Action
1	Launch the AirDefense GUI. *When connecting to AirDefense's GUI, administrators must enter the AirDefense Server's IP address in the following format:* **https://123.456.789.0:8543/wireless/wnapp.html**
2	Substitute the IP address you assigned to AirDefense with the address used in step 1 above.

Note: The addition of the "s" after the "http" instructs your browser to open an encrypted TLS connection with AirDefense's web AirDefense Server. The ":8543" that follows the IP address specifies the port number AirDefense uses for https connections.

Steps to Log On to a Remote AirDefense Server using the Command Line Interface

Step	Action
1	Launch your SSH client and connect to the AirDefense Server's IP address. ***Note:*** You must have at least version 2 of a SSH client installed on the remote workstation from which you wish to connect to the AirDefense Server.
2	At the logon prompt, enter the user name **smxmgr** and the unique password for your organization. *This connects you to the AirDefense Server.*
3	Enter the command **ADDadmin**--*the command is case-sensitive.* *This launches the Command Line Interface* *The ADDadmin screen appears*

See "Command Line Interface" on page 231 for instructions on using the ADDadmin utility.

1.4 Enhancing Client System Performance

This applies only if you are running the Microsoft® Internet Explorer® Browser.

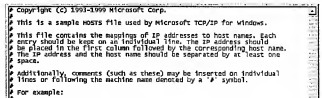
The AirDefense GUI is Java® Applet® based. You will see a noticeable performance increase in AirDefense from a Microsoft® Internet Explorer® Browser if you add the AirDefense Server to the Host file (in the root directory) of your operating system.

As a security check, Java applets perform reverse DNS lookups for any network connection for the purpose of obtaining both the IP address and the host name. Reverse lookups cause performance slowdowns that occur when the Applet tries to connect to an external AirDefense Server via proxy, and also because of the latency that results from a reverse lookup

1.4.1 Modifying the Host File

Steps to Modify the Host File

Step	Action
1	Go to your Host file root directory. *In Microsoft Windows, this is* ***C:\winnt\system32\drivers\etc\hosts,*** *or* ***C:\windowssystem32\drivers\etc\hosts***
2	Use Notepad or another text editor to add the IP address of the AirDefense Server to the Host file, and any name to be used as a reverse DNS name placeholder (for example, AirDefense2). See the example.
3	Save the file.

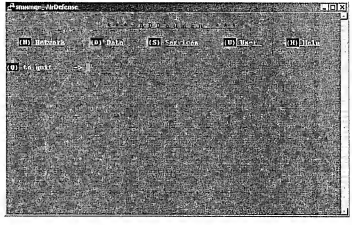


After Initial Tuning

During the next few weeks you should monitor traffic patterns using AirDefense. During this time, AirDefense will record information about the devices in your WLAN, and the data those devices transmit and receive. The data is available via AirDefense Reports (see Chapter 7, Reports). After reviewing this information, retune the performance policy thresholds for Stations and Access Points (see "Create Policy: Performance" on page 103). To receive more accurate alarms, set threshold values that reflect your normal network traffic patterns. Now AirDefense will only generate Performance alarms when wireless activity falls outside the normal range of activity.

1.6 Setting AirDefense Time, Date, Time Zone, and NTP

You must use the Command Line Interface to set the time, date, time zone, and NTP (time synchronization with a network server). You set the time, date, time zone, and NTP via the Date program on the ADDadmin screen.



> ***Note:*** If you are changing AirDefense time because, for example, you move the AirDefense Server's location from the east to west coast of the United States, you must also locate a *new* network time server in the same time zone.

Prerequisite: You should already be logged-in to the AirDefense Server, either locally or remotely, using the Command Line Interface (see "Logging On to the AirDefense Server" in this chapter). The ADDadmin screen must be in the terminal window.

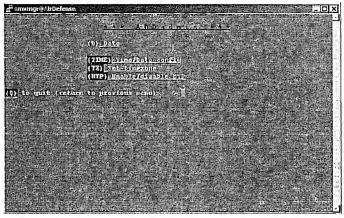
> ***Note:*** You may type any program command at the opening ADDadmin command prompt—it is not necessary to navigate first to the program page in order to execute a command within it. Whereas mis-typed commands in ADDadmin's secondary pages are forgiven, misspellings at the opening window log you out of the program.

1.6.1 Setting the Time/Date

Follow the steps below to set the time/date, time zone, and NTP.

Steps to Set the Time/Date

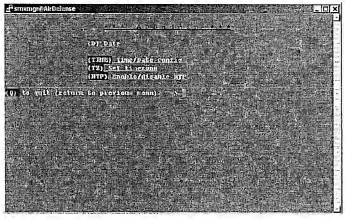
Step	Action
1	On the ADDadmin screen, type **d** at the command prompt to open the date settings program area. *The following screen appears.*



Step	Action
2	Type **time** to change the AirDefense Server's time and date. *The current date and time displays in bold text. You are prompted to enter a date in MMDDYYYY format. (Do not use colon, forward slash, or other delimiters.)*
3	Press **Enter.** *You are prompted to enter a time in 24-hour HHMM or HHMMSS format.*
4	Press **Enter.** *You are prompted to save your changes*
5	Type **yes** or **no.** *AirDefense reboots on exit from the ADDadmin.*

Steps to Set the Time Zone

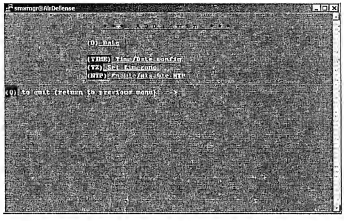
Step	Action
1	On the ADDadmin screen, type **d** at the command prompt to open the date settings program area. *The following screen appears.*



2	Type **tz** to change the AirDefense Server's time zone. *The Time zone screen displays a list of global, continental regions.*
3	Enter the corresponding number (to the left of your region name) and press **Enter**. *The next screen appears.*
4	Enter the abbreviation of your nationality (to the left of the nation) in which the AirDefense Server resides and press **Enter**. *The next screen appears.*
5	Enter the number of the region within your nationality in which the AirDefense Server resides and press **Enter**. ***Note:*** If you change the time zone, the following appears: *Changing timezone?* *Note that committing this change will immediately clear the database of all data and reboot the system upon exit of ADDadmin!!!* *Change timezone? (yes/no)*
6	Type **yes** or **no**. *Typing yes or no reboots and clears the database on exit from the ADDadmin.*

Steps to Enable or Disable NTP

Step	Action
1	On the ADDadmin screen, type **d** at the command prompt to open the date settings program area. *The following screen appears.*



2	Type **ntp** to enable automatic "time synching" with a network time AirDefense Server, and to specify the time AirDefense Server. *The NTP screen displays your current status in bold text—whether or not you are currently set to use NTP.*
3	Type **E** to enable NTP. *You are prompted to enter the IP address or fully qualified hostname (hostname.domainname.com) of a network time AirDefense Server.*
4	Type **D** to disable NTP. No additional input is required. *NTP is immediately disabled.*
5	To save the time AirDefense Server settings: type **Q** to quit this program *You are prompted to save your settings.*

Before you deploy a Sensor in your WLAN, you must do the following:

- Configure the Sensor's network settings
- Specify the Sensor's mode of operation. There are two configurations:
  - — Lock on Channel
  - — Scan Channels

Note: The default mode of operation is Lock on Channels 1, 6, and 11.

To configure the network settings and mode of operation for the Sensor, you must use the Sensor User Interface (Sensor UI). This interface resides on the Sensor, in an onboard HTML-based web server.

You must connect to the Sensor via a workstation or laptop, using a crossover Ethernet cable.You must also temporarily change the IP address and netmask on the workstation or laptop to match the Sensor's default network settings.

Note: For steps to upgrade the Sensor firmware, see Appendix C: Upgrading Sensor Firmware.

1.7.1 Physically Installing a Sensor

Follow the step below to physically install a Sensor.

Step to Physically Install a Sensor

Step	Action
1	Using a crossover Ethernet cable, connect each Sensor to the Ethernet port on your workstation or laptop. *On the Sensor side, the Ethernet cable plugs into the **ETHO port** on the back of the Sensor. This is the closest port to the power connector.*
2	Power up each Sensor.

1.7.2 Configuring Sensor Network Settings

Follow the steps below to configure the Sensor's network settings.

Steps to Configure Sensor Network Settings

Step	Action
1	Temporarily set your workstation or laptop IP address to **192.168.100.1** and subnet mask to **255.255.255.0.**
2	Enter **https://192.168.100.100** in your browser window. This is the default Sensor IP address. *Alternately, you can use **http** instead of https.* *You are prompted for a user name and password. The default values are:* *User Name: **admin*** *Password: **airsensor*** ***Note:*** You should change these logon value at the earliest opportunity. After logging onto the Sensor, input fields at the bottom of the Sensor Web Configuration page allow you to change the password.

3 Set the IP address of the AirDefense Server and network settings for your organization's network (see "Configuring Sensors" on page 19).

*Optionally, you can automatically receive setting from your DHCP AirDefense Server by selecting Yes on the **Use DHCP** toggle.*

Note: The web-based Sensor UI is nearly identical to the interface for Sensor configuration in the AirDefense GUI. There are two selections that you can only make from the Sensor UI: the **Sensor Active** configuration and **Security** settings. For more information, see "Configuring Sensors" on page 19.

1.7.3 Deploying Sensors

Follow the steps below to deploy Sensors in the wireless network.

Steps to Deploy Sensors

Step	Action
1	Install each Sensor at its deployment location.
2	Verify that the Sensor can connect back to the AirDefense Server.

To do this, use the AirDefense Server user interface to check the list of Sensors in the Sensor Manager (see "Sensor Manager" on page 63).

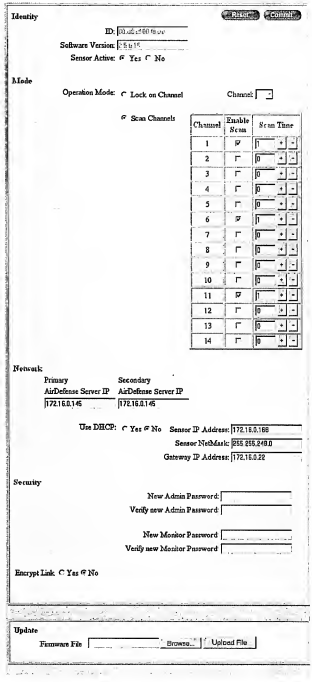
1.7.4 Configuring Sensors

Use the Sensor UI's Sensor Web Configuration screen to configure Sensors.

To configure Sensors, you must enter the appropriate information in each of the following categories.

- Identity
- Mode
- Network
- Security
- Update

The table on the next page describes the input fields on the Sensor Configuration screen.



Field	Meaning
Identity (Sensor identity)	• **ID:** This is auto detected. You cannot edit this field. • **Software Version:** This is auto detected. You cannot edit this field. • **Sensor Active** — **Yes:** Click **Yes** to place the Sensor online. When Yes, Sensor sends the AirDefense Server network traffic data — **No:** Click **No** to place the Sensor offline. When No, the Sensor does not communicate with the AirDefense Server (it is connected, but not sending data.)
Mode (Mode of Operation)	The following configurations determine the Sensor's operational modes. • **Lock on Channel:** Click this to lock the Sensor scan onto one channel. — **Channel:** Select the channel, 1-14, from the pull-down pick list. *Note:* Although the Sensor is configured to receive data on the selected channel, it may also receive data from adjacent channels, due to the overlapping nature of radio signals.This data also displays in the AirDefense GUI. See "Sensor Channel Scanning" on page 23 *Note:* The Sensor's default setting is to lock on channels 1, 6, and 11. **Scan Channels:** Click this if you want the Sensor to continuously scan one or more channels that you select, 1-14, and spend a length of time you define on each channel before moving to the next. — **Enable the Scan** for the selected channel by clicking the checkbox — **Configure the lengths of time** the Sensor should listen on them. You can either type a number, or use the plus and minus buttons in the "Scan Time" column to specify how long the Sensor should monitor the channel before jumping to the next one.)

Field	Meaning
Network (Settings)	The following configurations determine network connectivity. • **Primary AirDefense Server IP:** Enter the IP address of your primary AirDefense Server. The Sensor will send all its data to this address • **Secondary AirDefense Server IP:** Enter the IP address of your secondary AirDefense Server–*applies only if you are using more than one AirDefense Server.* The Sensor will send all its data to this address in the event connection is lost between the Sensor and the primary AirDefense Server. • **Use DHCP:** Optionally, you can use DHCP to assign an IP address to the Sensor. If DHCP is disabled, you must provide a valid IP address, netmask, and gateway IP address in order for the Sensor to communicate with the AirDefense Server — **Yes:** Click **Yes** to enable DHCP — **No:** Click **No** to disable DHCP. If you click No, you must provide a valid IP address, netmask, and gateway IP address in order for the Sensor to communicate with the AirDefense Server > **Sensor IP Address:** Enter a static IP address for the Sensor > **Sensor NetMask:** Enter the subnet to which the Sensor belongs > **Gateway IP Address:** You must provide the IP address of your gateway machine. (The Sensor must know how to get out to the Internet to send its data to the AirDefense Server.)

Field	Meaning
Security (Passwords and Encryption)	Use these fields to set and verify the passwords for an Administrator or a Monitor, and select data encryption. Passwords for both the Admin and the Monitor are case-sensitive. They may be up to 128 characters long, and may contain any alpha-numeric character. • **New Admin Password:** This password it the password for the Admin (Administrator). An administrator can **view and edit** configurations in the web-based Sensor UI, including changing or verifying the Admin and the Monitor password. The Administrator can change the password by entering a new one here. • **Verify new Admin Password:** Retype the Admin password for verification. • **New Monitor Password:** This password is for the Monitor. The Administrator must create or change this password here. A Monitor who logs on with this password may only **view** the data.The read-only user name is ***monitor.*** It cannot be edited • **Verify new Monitor Password:** The Administrator must retype the Monitor password here for verification. • **Encrypt Link:** — Click **Yes** if you want to encrypt the data between the Sensor and the AirDefense Server. Encrypted data uses port **443** to communicate with the AirDefense Server. — Click **No** if you do not want to encrypt the data between the Sensor and the AirDefense Server. Data that is not encrypted uses port **80** to communicate with the AirDefense Server.
Update (Firmware upgrade)	**Firmware File:** Use this field during a firmware upgrade. For complete upgrade instructions, see Appendix C: Upgrading Sensor Firmware. • Click **Browse** to navigate to the locally saved firmware file and select the upgrade file. • Click **Upload File** to automatically upgrade.

Scan Channels

There are only eleven transmission channels allowed by law in the U.S. However, since AirDefense does not transmit--it only passively scans--it allows you to scan all 14 channels specified by the 802.11b protocol and configurable in the wireless cards. AirDefense assumes that hackers will not be constrained by the eleven-channel legal restriction.

Because of the nature of radio transmission, a Sensor may receive overlapping signals from adjacent channels, even though you configured the Sensor to lock on a single channel. Some of AirDefense's reports on network traffic will report the data from adjacent channels in addition to the data from the selected channel.

Because radio signals overlap adjacent channels, most WLANs deploy two or more Access Points on channels as widely separated as possible—for example, on channels 1, 6, and 11. This is the default channel setting for AirDefense Sensors.You have two options for deploying AirDefense's Sensors: Dedicate one Sensor to listen to each Access Point, or, use one Sensor to monitor several Access Points. (If using one Sensor to listen to more than one Access Point, you configure it to scan the actual channels your Access Points are broadcasting on. You then define the number of minutes the Sensor scans each channel (i.e., monitor the Access Point's traffic on that channel) before switching to the next channel.

The results of AirDefense's channel scanning are displayed in AirDefense's Reports (see Appendix C, Reports). Statistics for each channel will only be available for the minutes the Sensor was actually scanning the channel.

2 Dashboard

The Dashboard Daily View displays a cumulative daily overview of AirDefense detection results. It is the first window that displays after you log on to the AirDefense Server.

Each day at midnight, AirDefense resets the previous day's statistics from the Dashboard window and begins collecting and displaying new data, updated once a minute, for the next 24 hours.

Use the Dashboard to view:

- The most recent alarms
- All identified Access Points
- Statistics about monitored channels
- The Stations generating the most alarms
- The Stations or Access Points that most recently violated wireless network policies

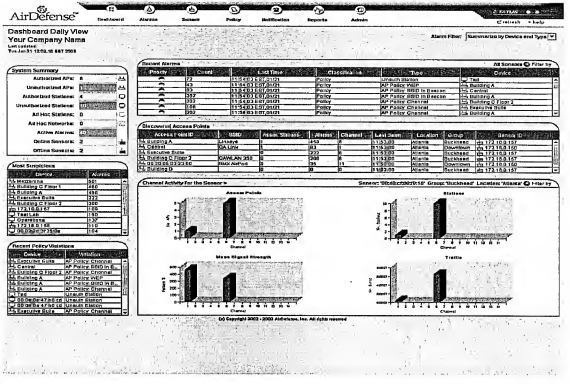
2.0.1 In This Chapter

This chapter contains the following topics.

2.0.2 Time Stamp

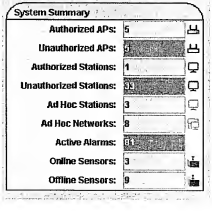
In the top-left corner of the Dashboard Daily View window, a on your local workstation reports when AirDefense last updated your browser's view of data

The graphic below shows a typical Dashboard Daily View screen.



2.1 System Summary

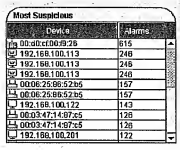
The System Summary table displays the following in the table below. Color-coded icons represent the states of Sensors, Access Points, and Stations in your WLAN. For more information on the icons and colors, see "Color-Coded Icons" on page viii.



Field	Description
Authorized APs	The number of authorized Access Points that have been operating since midnight.
Unauthorized APs	The number of authorized Stations that have been operating since midnight.
Authorized Stations	The number of unauthorized Access Points that have been operating since midnight. *Note:* If an originally unauthorized Access Point is later authorized, its count will be removed from this value.
Unauthorized Stations	The number of unauthorized Stations that have been operating since midnight. *Note:* If an originally unauthorized Station is later authorized, its count will be removed from this value. Any value greater than zero in this field will change the display to red.
Ad Hoc Stations	The number of ad hoc Stations with Ad Hoc Mode Enabled that have been operating since midnight in your enterprise. *Note:* Even a single Station that has not yet been joined by other ad hoc Stations can be detected because it will send out probes that look for a network, or beacons that advertise themselves as an ad hoc network.
Ad Hoc Networks	The number of ad hoc networks that have been operating since midnight in your enterprise. *Note:* An ad hoc network is one in which two or more Stations communicate directly with each other without the use of an Access Point.
Active Alarms	The number of active alarms that have been generated today (but not yet cleared by the administrator). *Note:* If *any* active alarm has a Critical priority, the count field will be red; if there are no Critical alarms, the count field will display the color of the highest priority alarm—orange for Major or yellow for Minor.
Online Sensors	The number of Sensors that are currently active (during the last minute).
Offline Sensors	The number of Sensors that are currently not active (during the last minute).

The Most Suspicious table displays the top fifteen Stations or Access Points that have the most uncleared alarms for the current day. You should take remedial action relative to the suspicious devices.

Note: To view alarm reports on all devices, see Chapter 7, Reports.



The Most Suspicious table contains the following information.

Column	Description
Device	Displays the color-coded icon and display identifier of fifteen Access Points or Stations that, since midnight, have generated the highest number of alarms. *Note:* You can determine how you want devices to display. See "Display Preferences for Device Identifiers" on page xvi.
Alarms	Displays the cumulative total of alarms the Station or Access Point triggered since midnight. This is updated once per minute.

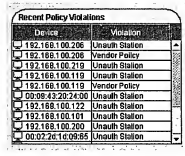
Double-click on any device display to go to the Alarm Manager (see "Alarm Manager" on page 39). The device display you select shows the alarms for the Station or Access Point to which the Device Identifier is assigned. The Alarms page shows details about each alarm.

AirDefense generates five categories of alarms:

- Policy
- Attack
- Event
- System
- Performance

Recent Policy Violations displays policy alarms—wireless network activity that violates policies established by your administrator.The table lists the Stations or Access Points that have generated the top fifteen most recent network policy violations—whose alarms have not yet been cleared.

Note: To view alarm reports on all devices, see Chapter 7, Reports.



The Recent Policy Violation table contains the following information

Column	Description
Device	Displays the color-coded icon and the Device Identifier of the fifteen Access Points or Stations that, since midnight, generated the fifteen *most recent* wireless network policy violations. ***Note:*** You can determine how you want devices to display. See "Display Preferences for Device Identifiers" on page xvi.
Violation	Identifies the specific policy the Station or Access Point violated. ***Note:*** This table only displays the most recent policy violations whose alarms have not yet been cleared.

Double-click on any device display to go to the Alarm Manager (see "Alarm Manager" on page 39), where the policy violation alarm is highlighted. From within the Alarms page, you may view details about the alarm, as well as the Location, Group, and Sensor information.

The Recent Alarms table displays information on alarms that are taking place today.

Whenever a Sensor detects that an Access Point or Station traffic contains characteristics of unauthorized traffic, it generates an alarm and displays the top fifteen most recent alarms in the Recent Alarms table. Once per minute, AirDefense refreshes the display of the fifteen most recent alarms that have not yet been cleared by the administrator.

Note: To view alarm reports on all devices, see Chapter 7, Reports.

Sensors and Alarms

Sensors continuously listen to all the wireless network traffic transmitted or received either on specified Access Points or on the channels specified by the administrator. All alarms are associated with a Sensor, a Group, and a Location.

Note: You must configure each Sensors's mode of operation see "Configuring Locations, Groups, and Sensors" on page 67 of Chapter 4, Sensor Manager.)

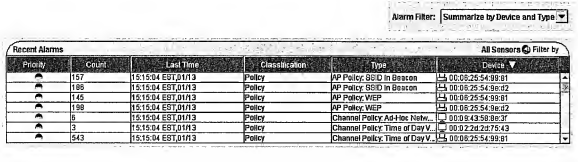
AirDefense detects and generates alarms when one of five types of network events occurs:

- Network traffic matches an intrusion signature (e.g., it detects multiple probe request messages after a Station has already associated with an Access Point)
- Network traffic uses disallowed protocols
- Network traffic is anomalous (e.g., falls outside normal network traffic patterns)
- Network traffic deviates from administrator-defined WLAN policies
- System-type alarms-something wrong with the Sensor

2.4.1 Filtering Recent Alarms

You can filter Recent Alarms by Location, Group, and Sensor. A **Filter By** icon at the top-right the Recent Alarms table enables you to access a Choose Sensor Set screen that displays individual Sensors, for all Sensors in a specific Location or Group, or all deployed Sensors.

An Alarm Filter pull-down enables you to choose how the alarm displays: for example, by Device, by Type, or by both.



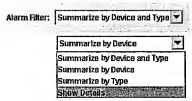
The table below describes the contents of each column.

Column	Description
(Alarm) Priority	A color-coded priority icon indicates the level of each Alarm. **Red** = Critical **Orange** = Major **Yellow** = Minor
Time	AirDefense records the timestamp when a network event generates an alarm, which is converted to your specific local system time (See "Date" on page 238 for information on changing AirDefense's clock.) While Dashboard's table of **Recent Alarms** displays a *one-line overview* of the alarm, you may see additional or related information about each by right-clicking anywhere on the row and selecting a navigation option. When Dashboard automatically refreshes its display once a minute, your "selection" will disappear.) Selecting one of the navigation options takes you either to AirDefense's Alarm Manager or Reports program areas, where information relevant to that alarm is displayed. (The options in the pop-up navigation window correspond, in part, to the filter options in the Alarm Manager.)
(Alarm) Classification	AirDefense generates five classifications of alarms: • **Policy**—generated when an Access Point or Station violates policies established in Policy Manager > Access Point and Policy Manager > Sensor. • **Attack**—generated when AirDefense detects wireless network traffic attempting to break network security. • **Performance**—generated when Access Points or Stations exceed network or traffic thresholds set in Policy Manager > Performance. • **System**—relates to the Sensor only. Generated when a subsystem of the AirDefense application reaches a critical threshold or ceases to perform as designed. • **Event**—generated when an Access Point changes mode. (See "Alarms" on page 55 for an annotated list of Alarms.)
Alarm (Type)	This column identifies the specific problem that generated the alarm. For example, the alarm-type AP Policy: WEP means that an Access Point Policy for WEP-usage was violated, and Station Assoc in BSS Exceeded means that a Station in the Basic Service Set exceeded the allowed number of associations with an Access Point. ("Alarms" on page 55 for an annotated list of Alarms.)
Device	If a Station or Access Point is responsible for generating the alarm, the **Device** column displays its Device Identifier. (Global CRC errors don't display a Device Identifier. Instead, it displays the Device Identifier of the Sensor it detects.)
Location	The Location name of the Sensor that is monitoring the alarms.

Column	Description
Group	The Group name of the Sensor that is monitoring the alarms.
Sensor	The Sensor that is monitoring the alarms.

Steps to Filter Recent Alarms

You can filter Recent Alarms by Location, Group, and Sensor. Follow the steps below to filter recent alarms.



Step	Action
1	Click on a summary type from the Alarms Filter pull-down.
2	Click on **Filter by** on the top right of the Recent Alarms table.

*The **Choose Sensor Set** screen appears. This displays a directory--the Sensor Tree View--of the individual Sensors, for all Sensors in a specific Location or Group, or all deployed Sensors. You configure this tree in Sensor Manager (see "Sensor Manager" on page 63.)*

3	Select a single Location, Group, or Sensor (or all Sensors).

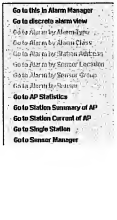
A Location, Group, or Sensor is selected when its name is highlighted. When a Location or Group is selected, all Access Points detected by the Sensors in that group will display.

4	Click **OK**.

Clicking OK will refresh the Recent Alarms table to display the most recent alarms for your selection.

2.4.2 Navigation Options

Right-click on an alarm in the **Recent Alarms** table to access a GoTo screen.



This screen has the following navigation options:

This Selection...	Takes You To...
Goto this in Alarm Manager	The Alarm Manager. The alarm you selected is highlighted in the table of alarms.
Goto discrete alarm view	The Alarm Manager. The alarm you selected is highlighted in the table of alarms.
Goto Alarm by Alarm Type	The Alarm Manager. The alarm you selected is highlighted in the table of alarms.The table of alarms is filtered to display only alarms of the type you selected, using Alarm Manager's *Alarm Type* filter.
GoTo Alarm by Alarm Class	The Alarm Manager. The alarm you selected is highlighted in the table of alarms.
GoTo Alarm by Station Address	The Alarm Manager. The alarm you selected is highlighted in the table of alarms. The table of alarms is filtered to display only alarms generated by the Station whose alarm you selected, using the Alarm Manager's MAC Address filter.
Goto Alarm by Sensor Location	The Alarm Manager. The alarm you selected is highlighted in the table of alarms. The table of alarms is filtered to display only alarms within the location where your selected alarm was generated, using Alarm Manager's *Sensor Set* filter.
Goto Alarm by Sensor Group	To the Alarm Manager. The alarm you selected is highlighted in the table of alarms. The table of alarms is filtered to display only alarms that were generated in the same Group as your selected alarm, using the Alarm Manager's *Sensor Set* filter.
Goto Alarm by Sensor	The Alarm Manager. The alarm you selected is highlighted in the table of alarms. The table of alarms is filtered to display only alarms generated by Stations or Access Points monitored by the Sensor reporting your selected alarm, using the Alarm Manager's *Sensor Set* filter.
Goto AP Statistics	The AP Statistics page, where you may view a summary of transmission statistics per minute for each Access Point on the network. This includes charts of the Access Points transmission bytes per hour, frames transmitted per hour, and frame size transmitted per hour. While not strictly related to the specific alarm, this may provide a contextual picture of the environment in which the alarm occurred
Goto Station Summary of AP	The Station Summary View page, where you may view a summary of transmission statistics for each Station that have taken place since a preset time, per Access Point, by report page. Reports include most active stations transmitting, most active stations receiving, observed stations, and new stations. While not strictly related to the specific alarm, this may provide a contextual picture of the environment in which the alarm occurred.

This Selection...	Takes You To...
Goto Station Current of AP	The Station Current View page, where you may view a current summary of statistics for each Station that is generating an alarm, by report page. The view shows the Access Point ID and Sensor ID associations with each alarm-generating Station. Reports include most active stations transmitting, most active stations receiving, observed stations, and new stations for Access Points, where you may view information about all the Stations currently associated with the Access Point that generated the alarm.
Goto Single Station	The Reports program area for Stations, where you may view minute-by-minute statistics about the Station and APs that generated the alarm
Goto Sensor Manager	The Sensor Manager, where the Sensor that reported the alarm is selected

Alternately, double-click on any column on the alarm's row—you are immediately transported to AirDefense's Alarm Manager, which will filter all alarms based on the value in the column you double-clicked.

> ***Example:*** *If you double-click in the Device column, the Alarm Manager page will display all alarms generated by that device, with the selected alarm at the top of the table. Of, if you double-click the Type column (and the alarm-type is AP Policy: rate violation), the Alarm Manager page will display all alarms that were AP Policy: rate violation.(If you double-click in the Priority, Time, or Classification columns, you are taken to the Alarm Manager page which displays all alarms.) Alarm Manager will auto-scroll to the specific alarm on which you double-clicked, and it will be highlighted in the table.)*

Double clicking in the Location, Group, and Sensor will take you to the Alarm Manager, filtered by the column you click.

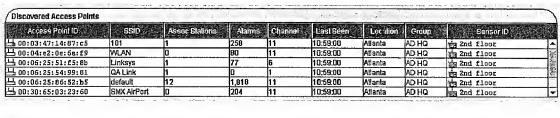
2.4.3 Discovered APs

The Discovered APs table displays the most recently seen (up to fifty) Access Points that have been active or detected since midnight. It also reports the Location, Group, and Sensor in which the Access Point was detected.

> ***Important:*** The most important data element in this table is the **Auth** (Authorized) column. A **Yes** or **No** in this column indicates the user-configurable authorization status of an Access Point. You should investigate any Access Point that is not authorized.

Unauthorized Access Points

Unauthorized Access Points might be newly deployed Access Points that you should now authorize. See "AP View" on page 94 in Chapter 5, Policy Manager for instructions on how to authorize, de-authorize, and ignore Access Points. Unauthorized Access Points can also be rogue Access Points illegally installed by your employees, or those deployed by a hacker.


Discovered Access Points

Access Point ID	SSID	Assoc Stations	Alarms	Channel	Last Seen	Location	Group	Sensor ID
00:03:47:14:87:c5	101	1	258	11	10:59:00	Atlanta	AD HQ	2nd floor
00:04:e2:0e:6a:f9	WLAN	0	80	11	10:59:00	Atlanta	AD HQ	2nd floor
00:06:25:51:f5:8b	Linksys	1	77	6	10:59:00	Atlanta	AD HQ	2nd floor
00:06:25:54:99:01	QA Link	1	0	1	10:59:00	Atlanta	AD HQ	2nd floor
00:06:25:86:52:b5	default	12	1,810	11	10:59:00	Atlanta	AD HQ	2nd floor
00:30:65:03:23:60	SMX AirPort	0	204	11	10:59:00	Atlanta	AD HQ	2nd floor

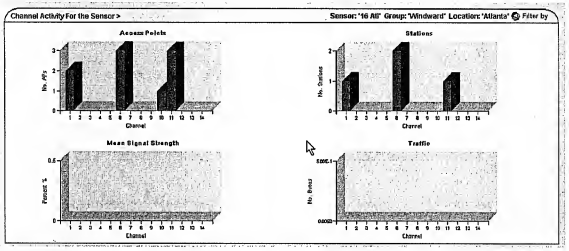
The Discovered Access Points table contains the following information.

Column	This Column...
Access Point ID	Displays the color-coded icon and the Device Identifier of each Access Point detected since midnight. ***Note:*** You can determine how you want devices to display. See "Display Preferences for Device Identifiers" on page xvi.
SSID	If AirDefense can determine it, this column displays the name of the Extended Service Set (i.e., the SSID) broadcast by the Access Point. The wireless network industry inconsistently names the "Service Set Identifier," sometimes calling it an "SSID" and other times calling it an "ESSID" (the "E" stands for extended). AirDefense uses "SSID" as the name given to a particular wireless network. On a related note, we recommend—as a security precaution—that generally, SSIDs should not be broadcast "in the clear," and that secure authentication procedures be used for Stations trying to associate with the Access Point. Consider creating a policy (in **Policy Manager>Create Policy>Configuration**) that generates an alarm whenever AirDefense hears an Access Point broadcasting its SSID. Select **No** for Allow SSID In Beacon.
Assoc Stations	This columns displays the number of Stations *currently* associated with each Access Point.
Alarms	This column displays the cumulative total of alarms (that have not been cleared by the administrator) generated either by the Access Point or any Station associated with it since midnight. Every item in the Dashboard updates once per minute.
Channel	This column displays the advertised channel over which the Access Point is currently transmitting and receiving data.
Last Seen	This column displays the hour and minute when the Access Point was last seen by a Sensor.
Location	This column reports the Location of the Access Point.
Group	This column reports the Group to which the Access Point belongs.
Sensor ID	This column reports the Sensor that is detecting the Access Point. (In some cases, two or more Sensors may detect the same Access Point. The one reported here is the Sensor that detects it with the strongest signal.)

Double-clicking on any Access Point in the table transports you to the Policy: Access Point program area where you may "zoom in" on details of that Access Point's policy configuration for review or editing. Right-clicking on any Access Point in the table opens a pop-up navigation window allowing you to jump to the Policy: Access Point or Reports: Access Point Statistics page, or the Sensor Manager page for the Sensor that discovered the Access Point. (The Access Point page lets you see details of the Access Point's configuration and policies applied. The AP Statistics page displays a minute-by-minute report of network traffic statistics for that Access Point).

The Channel Activity for the Sensor table displays a variety of graphs that show statistics for the channels over which a Sensor detected network traffic. The graphs display data one Sensor at a time--the Sensor Device Identifier, Group, and Location display on the top right of the table. The graphs are as follows:

- Access Points
- Stations
- Mean Signal Strength
- Traffic



2.5.1 Viewing Sensor Channel Activity

Follow the steps below to view a Sensor's channel activity.

Note: Sensor Selection defaults to display the first Sensors on the list.

Steps to View a Sensor's Channel Activity

Step	Action
1	Click on **Filter by.** *The Choose A Sensor screen appears. This displays the Sensor program tree. You configure this tree in Sensor Manager (see "Sensor Manager" on page 63.)*
2	Select a single Sensor. *A Sensor is selected when its name is highlighted.*
3	Click **OK.** *Clicking OK will refresh the Channel Activity for the Sensor table to display the statistics for your selection.*

AirDefense generates alarms for five classifications of wireless network activity, and prioritizes each alarm as critical, major, or minor.

3.1.1 Alarm Classifications

The table below lists the alarm classifications.

Alarms	Description
Policy Alarms	Policy Alarms generate when an Access Point or Station violates wireless network policies. Administrators create policies for how the individual Access Points should behave in Policy > Access Point. Policies for "time-of-day" wireless network access and ad hoc networks are created in Policy > Sensor. If AirDefense detects deviations from these policies, alarms are generated.
Attack Alarms	Attack Alarms generate when AirDefense detects wireless network traffic attempting to break network security. AirDefense captures and analyzes the Layer 1 and Layer 2 air-packets. AirDefense's state analysis engine and multi-dimensional detection engine are designed to monitor WLAN traffic for: questionable signatures, policy deviations, inconsistent protocols, and statistical anomalies.
Performance Alarms	Performance Alarms generate when Access Points or Stations exceed configurable network or traffic thresholds. Administrators set a variety of thresholds (such as signal strength levels, numbers of Station-to-Access Point associations, and bytes of data transmitted) in Policy > Performance.
Events Alarms	Events Alarms generate when there are unexpected changes in the way Access Points operate.
System Alarms	System alarms generate when AirDefense devices fail to perform as designed.

3.1.2 Alarm Priorities

In addition to generating four classifications of alarms, AirDefense prioritizes them as:

- **Critical** alarms—those that should receive immediate attention
- **Major** alarms—those suggestive of potentially serious problems
- **Minor** alarms—those that suggest potential problems

Color-Coded Number Fields

At the top of the Alarm Manager screen are seven color-coded number fields. The data in these fields updates once per minute.

The table below describes the meaning of each field.

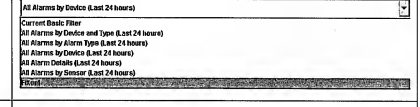
Field	Meaning
Total	Shows the cumulative total of *all* alarms generated over the past 30 days. (When alarms are 30 days old they are deleted from AirDefense's database.)
Critical	Shows the cumulative total of **critical** alarms generated in the past 30 days that have not been cleared.
Major	Shows the cumulative total of **major** alarms generated in the past 30 days that have not been cleared.
Minor	Shows the cumulative total of **minor** alarms generated in the past 30 days that have not been cleared.
Cleared	Shows the number of alarms that have been generated in the past 30 days and have been cleared (indicating that the administrator has resolved the problem generating them).
New	Shows the number of alarms that generated since the **Refresh** button was last clicked.
Changed	Shows the number of alarms whose cleared or acknowledged status was changed by any administrator logged onto AirDefense from any browser while you were viewing the current page of alarms, including those that you, as the current user, have cleared or acknowledged. (Clicking **Refresh** will reset the value in the **Changed** field to zero.)

You can determine how you would prefer to view the alarms that the AirDefense Server generates.

An Alarm Filter Settings screen above the **Alarms** table lets you filter your view of the alarms. You can use the built-in (default) filters, or you can form your own custom filters. You must set filters for every AirDefense Server in your WLAN.

Using filters effects how alarms display in the Alarms table.

The table below lists the fields in the Alarm Filter Settings screen.

Field	Meaning
Filter	This field allows you to choose one of the built-in, or already configured filter settings that determines how you view alarms. Alternately, you can form your own filter, using Alarm Manager's filter editing features. 
Basic 	Click Basic to access the Basic Filter Editor screen. This screen enables you to run a basic filter. You can determine the detail level of filters (if and how alarms are summarized and which columns display); limit alarm queries to devices; and determine the time range for the report, for example, the last 24 hours.
Advanced 	Click Advanced to access the Advanced Alarm Filter Editor screen. This screen enables you to edit existing filters, add a new filter, copy a filter, or delete a filter.
Critical Alarms	Click Critical Alarms to display only alarms that have a priority of Critical. 
Major Alarms	Click Major Alarms to display only alarms that have a priority of Major. 
Minor Alarms	Click Minor Alarms to display only alarms that have a priority of Minor.

Field	Meaning
Show	**All:** Click All to display both Active and Cleared alarms. **Active:** Click Active to display active alarms only. **Cleared:** Click Cleared to display cleared alarms only.
Interval	Choose a built-in time interval for viewing the alarms, or an interval based on the time you configured in a filter. If you choose Custom Time Range, you can configure the **From** and To dates and times you would like to view alarms. 

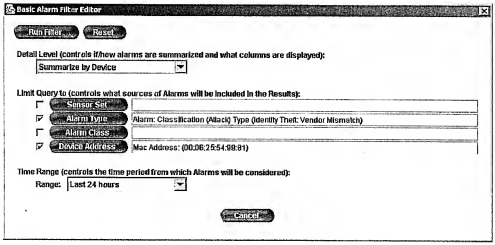
Use the Alarm Manager's filter editing features to select a built-in (default) filter or form your own custom filters. The filter determines how the Alarm table displays an alarm.

To edit filters, you can use two screens. These are:

- Basic
- Advanced

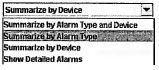
3.2.1 Basic Filter Editing

The Basic Filter Editor enables you to run a basic filter. You can determine the detail level of filters, limit alarm queries to devices; and determine the time range for the alarm report. You cannot use Basic Filter Editor to Add, Copy, or Delete filters. To do this, see " on page 48.



Steps to Use the Basic Filter Editor

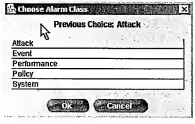
Step	Action
1	Access the Basic Filter Editor by clicking on Basic on the Filter Settings Screen. *The Basic Alarm Filter Editor screen appears.*
2	Choose a summary from the pull-down.
3	Make one or more selections to limit your query to devices. Click one or more of the following.



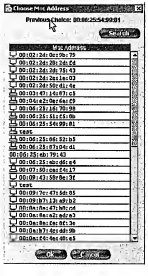
Note: You can choose either Alarm Class or Alarm Type, but not both.

- Click on **Sensor Set** if you would like to limit your query by Sensor. The Choose Sensor Set screen appears. Choose Sensors from screen and click **OK**. This screen also has a search utility.
- Click on **Alarm Type** if you would like to limit your query to Alarm Type. The Choose Alarm Type screen appears. Choose Alarm Types from the screen and click **OK**. This screen also displays the classification, and shows the previous choice, if any. It also has a search utility.

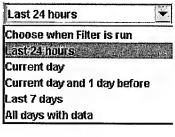
- Click on **Alarm Class** if you would like to limit your query to Alarm Class only. The Choose Alarm Class screen appears. Choose Alarm Classes on the screen and click OK. This screen shows the previous choice, if any. It also has a search utility.



- Click **Device Address** if you would like to limit your query to the MAC address of a device. The Choose MAC Address screen appears.The screen displays your previous choice, and provides a Search utility.



4 Enter a time range for running the filter, from the pull-down list. If you do not choose a time, the filter runs at the AirDefense default--**Last 24 hours.**



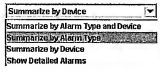
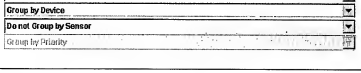
5 When you are finished configuring the screen, click **Run Filter** to run the filter. The Alarm screen displays your filtered alarms.

Alternately, you can click Reset to clear all changes from the screen.

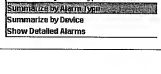
Cancel leaves the screen without changes.

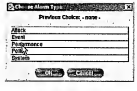
Currently Applied Filter

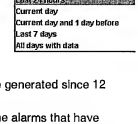
Resting your mouse over either the Basic or the Advanced buttons on the Alarms Filter Screen brings up a Currently Applied Filter information screen. This screen displays information about the currently applied filter.

Item	Displays...
Name	The name of the filter.
Detailed Level	The Detail Level you chose. In Basic Filter Editing:  In Advanced Filter Editing:
Summarized by	How you limited your query. 
Showing	How you chose to group your alarms. 
Limited View to Alarms	The time range you chose. 

The table below describes the fields in the Basic Alarm Filter Editor

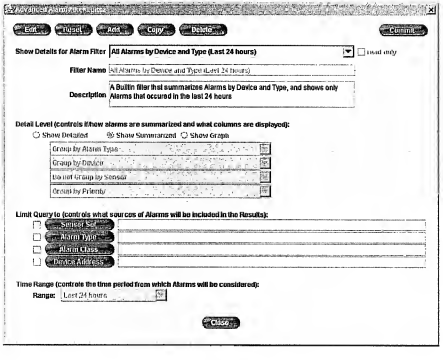
Field	Meaning
Detail Level	The Detail Level controls if alarms are summarized, and how they display in the Alarms screen. 

Field	Meaning
Limit Query 	• **Sensor Set:** Click **Sensor Set** to access the Choose Sensor Set screen. Use the screen to limit your query to all Sensors in a Location or Group, or an individual Sensor in your WLAN.The screen provides a Search utility. Click on **Filter by** to access the same screen.  • **Alarm Type:** Click **Alarm Type** to access the Choose Alarm Type screen. Use the screen to limit your query to alarm type (also displays alarm classification. The screen displays your previous choice, and provides a Search utility. • **Alarm Class:** Click **Alarm Class** to access the Choose Alarm Class screen. Use the screen to limit your query to alarm classification only.    • **Device Address:** Click **Device Address** to access the Choose MAC Address Screen. Use the screen to limit your query to MAC address. The screen displays your previous choice, and provides a Search utility. 

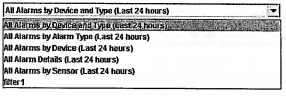
Field	Meaning
Time Range	Controls the time range from which the Alarms display. The AirDefense default is the **Last 24 hours**.  • **Choose when filter is run:** • **Last 24 hours (default):** Displays the alarms that have generated in the last 24 hours. • **Current day:** Displays the alarms that have generated since 12 midnight of the current day. • **Current day and 1 day before:** Displays the alarms that have generated since 12 midnight of the current day, plus the 24 preceding hours. • **Last 7 days:** Displays the alarms that have generated in the last seven days. • **All days with data:** Displays all alarms on hand for all of the days AirDefense has been in operation up to the current day. Days end at 12 midnight. This can be for a maximum of thirty days.

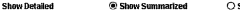
3.2.2 Advanced Filter Editing

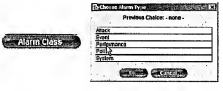
The Advanced Filter Editor screen enables you to Add, Copy, and Delete filters. It also enables you to display filters at a greater level of detail than the Basic Filter Edit. You can determine the detail level of filters, limit alarm queries to devices; and determine the time range for the alarm report.



The table below lists the fields in the Advanced Filter Editor.

Field	Meaning
Show Details for Alarm Filter	Select the filter you want to edit or copy from the pulldown list. You cannot edit built-in (default) filters 
read only	When this checkbox has a check, it indicates that an administrator has marked this filter as read only. You cannot edit this filter.
Filter Name	The name of the filter you selected in the Show Details for Alarm Filter pull-down.
Description	A description of the filter

Field	Meaning
Detail Level	The Detail Level controls if alarms are summarized, and how they display in the Alarms screen (also see "Alarm Detail Levels" on page 52).  Choose one: • **Show Detailed:** Click this to show all alarm details. • **Show Summarized:** Click this to show summaries of the alarms, for example, by either Type or Class. • **Show Summarized as Graph:** Click this to show a summary of the alarms as a graph. If you choose Show Summarized or Show Summarized as Graph, you can further specify what displays using the alarm Type or Class, Device, and Sensor pull-downs.  • **Type or Class** — Do not Group by Alarm Type or Class — Group by Alarm Type — Group by Alarm Class • **Device** — Group by Device — Do not Group by Device • **Sensor:** — Do not Group by Sensor — Group by Sensor — Group by Sensor Group — Group by Sensor Location • **Priority** You may click on one or any combination of the following: — **Critical Alarms:** Check this to display Critical alarms. — **Major Alarms:** Check this to display Major alarms. — **Minor Alarms:** Check this to display Minor alarms.

Field	Meaning
Limit Query 	• **Sensor Set:** Click **Sensor Set** to access the Choose Sensor Set screen. Use the screen to limit your query to all Sensors in a Location or Group, or an individual Sensor in your WLAN. The screen provides a Search utility. Click on **Filter by** to access the same screen.  • **Alarm Type:** Click **Alarm Type** to access the Choose Alarm Type screen. Use the screen to limit your query to alarm type (also displays alarm classification. The screen displays your previous choice, and provides a Search utility. • **Alarm Class:** Click **Alarm Class** to access the Choose Alarm Class screen. Use the screen to limit your query to alarm classification only.   • **Device Address:** Click **Device Address** to access the Choose MAC Address Screen. Use the screen to limit your query to MAC address. The screen displays your previous choice, and provides a Search utility. 

Field	Meaning
Time Range	This sets the time range for your filter. The choices are as follows: **Time Range (controls the time period from which Alarms will be considered):** **Range:** Last 24 hours • **Choose when filter is run:** • **Last 24 hours (default):** Displays the alarms that have generated in the last 24 hours. • **Current day:** Displays the alarms that have generated since 12 midnight of the current day. • **Current day and 1 day before:** Displays the alarms that have generated since 12 midnight of the current day, plus the 24 preceding hours. • **Last 7 days:** Displays the alarms that have generated in the last seven days. • **All days with data:** Displays all alarms on hand for all of the days AirDefense has been in operation up to the current day. Days end at 12 midnight. This can be for a maximum of thirty days.

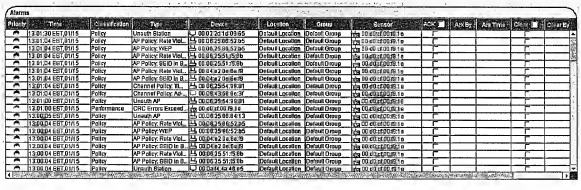
Alarm Detail Levels

Detail Level controls if alarms are summarized, and how they display in the Alarms screen.

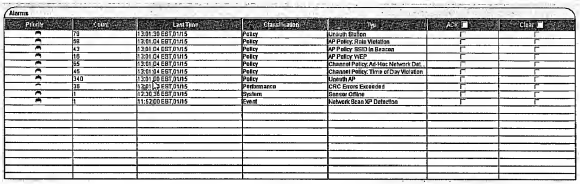
○ Show Detailed ◉ Show Summarized ○ Show Summarized as Graph

Choices--*you can choose one*:

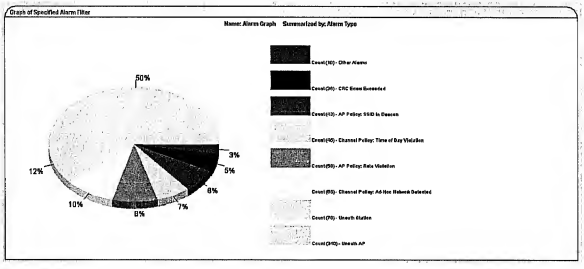
Show Detailed: Click this to show all alarm details. Below is an example display.



Show Summarized: Click this to show summaries of the alarms, for example, by either Type or Class. Below is an example display.

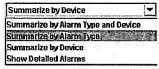
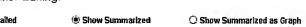
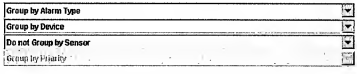
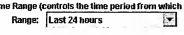


Show Summarized as Graph: Click this to show a summary of the alarms as a graph. Below is an example display.



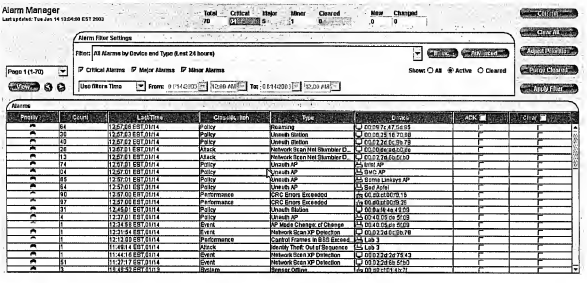
Currently Applied Filter

Resting your mouse over either the Basic or the Advanced buttons on the Alarms Filter Screen brings up a Currently Applied Filter information screen. This screen displays information about the currently applied filter.

Item	Displays...
Name	The name of the filter.
Detailed Level	The Detail Level you chose. In Basic Filter Editing:  In Advanced Filter Editing: 
Summarized by	How you limited your query. 
Showing	How you chose to group your alarms. 
Limited View to Alarms	The time range you chose. 

Alarms displays every alarm generated for the past 30 days. AirDefense displays up to 100 alarms at a time (scroll down to see the entire list).

Important: The Alarms table summarizes alarms by different criterion.The filter you choose determines the columns that display in the Alarms table. In all views, the **Ack By** and **Clear** column is always present, which allows you to acknowledge and clear the alarm.

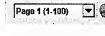


3.3.1 Using Alarms

Follow the steps below to use Alarms

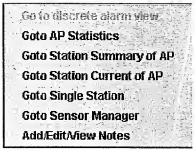
Steps to Use the Alarms

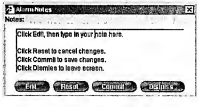
Step	Action
1	To scroll through the pages, select a page from the **Page** pick list at the top-left of the table.
2	Click **View Page**, or click the left or right browse buttons.
3	To update the Alarms table, click **Refresh** in the upper right corner of the screen



The table populates with alarms, based on the filter you selected.

Right Click--Place your mouse over any single entry in the table and right click. A **Goto** *screen appears that you can use to go directly to the report summaries in Reports (see Chapter 7, Reports).*



Goto	Takes you...
Go to discrete alarm view	To the most recent view in the Alarms screen, based on the last filter selection.
Goto AP Statistics	To the AP Statics screen in Reports.
Goto Station Summary of AP	To the Station Summary screen in Reports.
GoTo Station Current of AP	To the Station Current View screen in Reports.
Goto Single Station	To the Single Station View screen in Reports.
Goto Sensor Manager	To Sensor Manager
Add/Edit/View Notes	To The Alarm Notes sub-screen of the current alarm (see "Alarm Details" on page 62). 

Alarms displays the following:

Column	Description
Priority	A color-coded priority icon indicates the level of each Alarm. **Red** = Critical **Orange** = Major **Yellow** = Minor
Time	Time the alarm was generated, converted to your local time.

Column	Description
Classification	Alarm classification. The categories are: • **Policy** • **Attack** • **Performance** • **Event** • **System**
Type	This column identifies the specific type of alarm that generated the alarm. For example, the alarm-type "AP Policy: WEP" means that an Access Point Policy for WEP-usage was violated, and "Station Assoc in BSS" means that a Station in the Basic Service Set exceeded the allowed number of associations with an Access Point. (Appendix A, Reports, on page 245 for an annotated list of AirDefense Alarms.)
Device	Color-coded icon and Device Identifier of the offending Access Point or Station. *Note:* Holding the mouse over the field brings up a rollover screen that shows the Device Identifier of the Access Point or Station. *Note:* If the alarm is not generated by a Station, the Station Address field will contain the Device Identifier of the reporting Sensor.
Location	The Location name of the Sensor that is monitoring the alarm.
Group	The Group name of the Sensor that is monitoring the alarm.
Sensor	Color-coded icon of the Sensor that reports the alarm. *Note:* Holding the mouse over the field brings up a rollover screen that shows the Device Identifier of the Sensor.
Ack	Click this checkbox if you are an administrator and you want to acknowledge that you have seen this alarm. • When you select this checkbox, the Ack By and Ack Time fields are automatically filled with your AirDefense logon name and the current time. • AirDefense does not write this acknowledgment to its database until you click **Commit** at the top of the page.
Ack By	Logon name of the person who acknowledged the alarm.
Ack Time	Timestamp when the alarm was acknowledged. *Note:* This field displays Pending until the changes have been written to the database.

Column	Description
Clear	Click this checkbox if you wish to hide an alarm from view after the situation that generated it has been resolved. (When you select this option, the Ack check box is also checked, and your logon name and the current time are automatically entered in the Ack By and Ack Time fields.) • AirDefense does not write this information to its database until you click Commit at the top of the page. • After checking the Clear check box and clicking Commit, the cleared alarms will be hidden from view unless the state filter is set to All. • To clear all alarms on the current page, click the Ack or Clear boxes at the top of the column, then click **Commit**. • To clear all alarms on all pages, click Clear All.To undo any changes to alarm status prior to clicking **Commit**, click **Undo**.
Clear By	This column displays the logon name of the person who cleared an alarm.
Clear Time	This column displays the timestamp when an alarm was cleared. It displays "Pending" until the changes have been written to the database
Notes	Use this field to add notes (comments) to alarms (see "Using Notes" on page 59). Adding notes can help you isolate a configuration problem or suspect activity, especially if the alarms occur in different geographical locations.

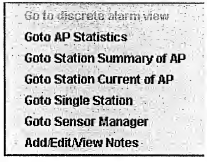
3.3.2 Using Notes

Steps to Use Notes

Step	Action
1	Right click your mouse on Notes column that corresponds to the alarm.

The Notes pick list appears.

Alternately, you can use the Notes pick list to ***GoTo*** *the report summaries, in the Reports program area*



2 Select **Add/Edit/View Notes.**

3 The Alarm Notes subscreen appears.

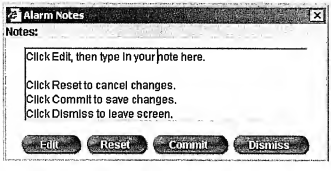
4 To add a note:

- Click **Edit** and enter the text into the screen.

  You can click ***Reset*** *at any time to remove your note entries without saving.*

  You can click ***Dismiss*** *at any time to leave the Alarm Notes screen without saving your note entries.*

- Click **Commit** to save the note.

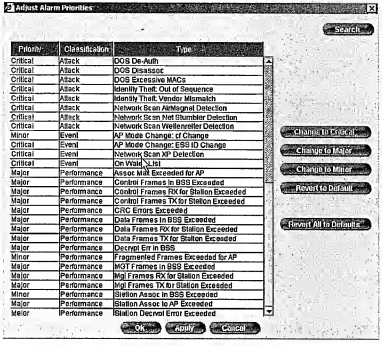


5 To leave the screen, click **Dismiss.**

The Confirm Discard screen appears. Click on ***Yes*** *or* ***No.***

3.3.3 Adjusting Alarm Priorities

Use the Adjust Priorities feature to group alarms by priority (Critical, Major, and Minor). This feature enables you to change the alarm priority levels of any alarm.



Steps to Adjust Alarm Priorities

To adjust alarm priorities, do the following:

Step	Action
1	Click the **Adjust Priorities** button on the right of the main Alarm Manager screen.  *An Adjust Alarm Priorities screen displays.*
2	Select the alarm you wish to change.
3	Click the appropriate button to change alarm priorities: *Click **Change to Critical** to change the priority to Critical* *Click **Change to Major** to change the priority to Major.* *Click **Change to Minor** to change the priority to Minor.* *Click **Revert to Default** to change the individual alarm back to its default value.* *Click **Revert all to Default** to change all listed alarms back to their default values.*
4	After making changes, Click **Apply** to view all changes.
5	Click **OK** to Save all Changes *Alternately, you can click **Cancel** to cancel all changes.*
6	Click **Commit** on the main Alarm Manager screen.

The table below describes columns in the Adjust Alarm Priorities screen.

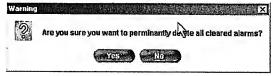
Column	Meaning
Priority (Alarm priority)	The priority of the alarm--Critical, Major, or Minor. For more information, see "Alarm Priorities" on page 41.
Classification (Alarm class)	The classification of the alarm--Policy, Attack, Performance, Events, System. For more information, see "Alarm Classifications" on page 40.
Type (Alarm type)	Type of violation that is occurring.

3.3.4 Purging Cleared Alarms

Use the Purge Cleared feature to purge cleared alarms from AirDefense.

Steps to Use Purge Cleared

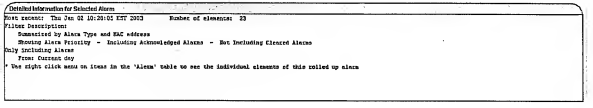
Step	Action
1	Click on the Purge Cleared button. *A Warning screen appears.*
2	Click **Yes** to purge all cleared alarms from AirDefense. *Alternately, you can click No to return to the Alarms screen without changes.*



The Detailed Information for Selected Alarms table displays information about selected alarms in the Alarm table. The details change, depending on the type of alarm you select.

Using your mouse, you can do a text capture of the information in this table, and save it to another location on your workstation.

To view the details of an individual alarm, select an individual alarm in the Alarm table. (See "Alarms" on page 55. for information on each alarm.)



4 Sensor Manager

Use Sensor Manager to configure individual Sensors for Identification, network accessibility, and mode of operation, and to define the AirDefense hierarchy, consisting of the following:

- System
- Location
- Group
- Sensor
- Access Point
- Station

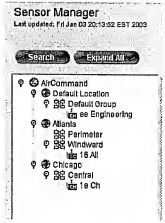
4.0.1 In This Chapter

This chapter contains the following topics.

Distributed Network Architecture

AirDefense's unique design enables it to protect enterprise environments that cover a large amount of geographical territory. A single AirDefense Server receives real-time data from widely-deployed Sensors via Internet, WLAN or LAN. You can deploy more than one AirDefense system in high bandwidth environments.

The left side of the Sensor Manager window shows the Tree View of your network



> *Note:* Until you create your own Groups and Locations, only the top level (system) icon and a location named "Default" appears on the tree. The Default location contains one group, also named "Default." You cannot delete the default Location and Group.

While you can manually create Locations and Groups in Tree View, you do not manually add Sensors. Sensors are *automatically* added to this tree when you the AirDefense Server receives their data--*after you configure and add the Sensor to your WLAN*. As each new Sensor comes online, it is automatically placed in the Default Group in the Default Location. You do not *have* to create Locations and Groups—there is no necessary reason why Sensors must be moved out of Default. Your administrator creates the organizational structure.

4.1.1 Color-Coded Icons

The table below lists the color-coded icons that appear in Sensor Manager Tree View.

Color	Meaning
	Magnifying Glass. Whenever a Location or Group contains devices, this icon displays to the left of the Location or Group.This indicates that the Location or Group can expand or collapse. Expanding reveals the Sensors, Access Points, and Stations that belong to the Location and Group.
	This is the highest level in the tree, representing the AirDefense Server.
	This is the second highest level in the tree, representing the Sensor Location. Expand the Locations to expose the individual Sensors.
	This is the third highest level in the tree, representing the Sensor Group. Expand the Locations to expose the individual Sensors.
	Red indicates that the Sensor is offline, i.e., not in communication with the AirDefense Server. *Note:* If you did not intentionally take a Sensor offline, check the Sensor's configuration settings (see "Installing and Configuring a Sensor" on page 17.

Color	Meaning
	Green indicates that the Sensor is online, functioning normally, and in communication with the AirDefense Server. *Note:* Because the Sensor Manager page is not automatically updated, the Sensor's color only represents its status at the moment the page was opened. Click **Refresh in** the upper right to refresh the data.)
	Blue indicates that Sensor is not being physically observed by the AirDefense Server.

A letter can exist inside each Sensor's icon:

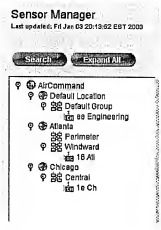
Letter	Meaning
	Sensor is in **Lock on Channel** mode
	Sensor is in **Scan Channels** mode

4.1.2 Navigating the Sensor Manager Tree View

Below are some helpful tips for navigating the Sensor Manager Tree View.

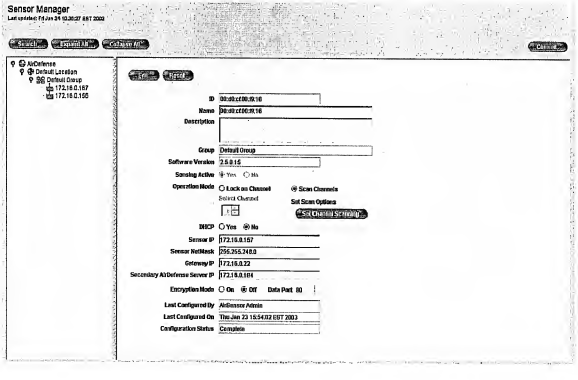
Right-click on the System (your company) or any Location, Group, or Sensor in the Sensor Manager Tree View--this brings up a menu that you can use to select Locations, Groups, and Sensors.

- Click on the System (your company) icon to add a Location.
- Click on a Location to add a Group or delete the Location. (You may not delete a Location until all Groups within it have first been deleted.)
- Click on a Group to delete the Group, or move it to a new Location. (You may not delete a Group until all Sensors within it have first been deleted or moved to another group). If you select Change Location, a small window presents a pick list of all your existing Locations. Selecting the new Location and clicking **OK** immediately moves the group to the new Location.
- Select multiple items in the tree (<Ctrl>click or <Shift> click) to move all the selected groups to another Location.
- Click on a **single** Sensor to delete the Sensor or move it to another Group. If you select Change Group, a small window displays a directory of all your existing Groups. Select the new Group and click **OK**--the Sensor immediately moves to the new Group.
- Use <Ctrl>click or <Shift> click to select multiple Sensors. You can move all the selected Sensors to another Group, or delete them.



Whenever you create a Location or Group, or click on an existing Location, Group, or Sensor in the tree, input fields appear to the right of the tree that enable you to name the selection, provide descriptive text, as well as set other options. (See "Configuring Locations, Groups, and Sensors" on page 67 for more information.

Example: *Below is the screen that appears when you click on an individual Sensor in the tree. This screen enables you to configure the Sensor.*



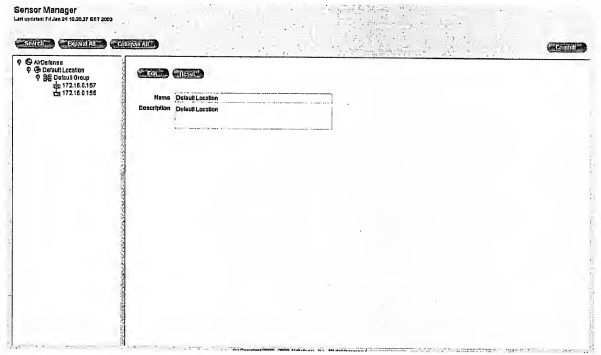
Click on an individual Location, Group, or Sensor in the Sensor Tree View to display the configuration screen for each.

4.2.1 Configuring Locations

Locations are the top-level descriptors. Depending on the size of your wireless network, Locations (represented by a "globe" icon) can denote a cluster of buildings, or even a city, containing any number of offices. Below Locations on the hierarchy are Groups (represented by an icon of multiply-connected Sensors).

When you select a Location icon, a screen appears with input fields that enable you to provide a name and description of the Location. **Names must be unique**, and a maximum of 15 characters.

Note: The name of the default location cannot be changed.



Steps to Add a Location to AirDefense

Step	Action
1	To add a Location, place your mouse over the system (top) icon in the Sensor View Tree and right click. *The Add Location selector appears.*
2	Click on the **Add Location** selector. *A new location configuration screen appears on the right.* *A new location placeholder appears on the Sensor View Tree.*

3 Enter a Name and **Description** for the new location. **Names must be unique**, and a maximum of 15 characters.

(If you click any other tree icon before saving your changes, AirDefense will prompt you to save them.) Click **Reset** *to undo unsaved edits.*

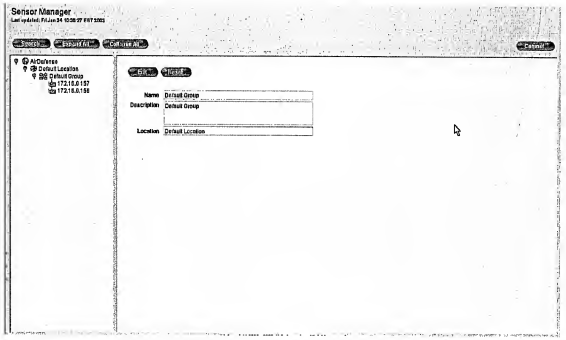
4 Click **Commit.**

Steps to Edit a Location in AirDefense

Step	Action
1	Click on an existing Location in the Sensor View Tree. *The Edit location screen appears on the right with the name and description of the Location in the Name field.*
2	Click **Edit** to edit the field. *(If you click any other tree icon before saving your changes, AirDefense will prompt you to save them.) Click* **Reset** *to undo unsaved edits.*
3	Click **Commit.**

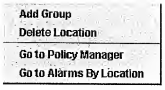
4.2.2 Configuring Groups

Groups denote clusters of individual Sensors, with each Sensor monitoring the activity of one or more Access Points. Beneath Groups are the Sensors, represented by a Sensor icon.



Steps to Add a Group in AirDefense

Step	Action
1	To add a Group, place your mouse over the Location icon in the Sensor View Tree and right click. *The Add/Delete Group selector appears.*
2	Click on **Add Group** to add a Group. *A new group configuration screen appears on the right.* *A new group placeholder appears on the Sensor Tree View.*
3	Enter a (Group) **Name** and **Description** for the new Group. Names must be unique, and a maximum of 15 characters. ***Note:*** The Location to which the Group belongs may not be edited in this screen—to change a Group's Location, right-click on the Group object in the Tree View and select **Change Location**. ***Note:*** You cannot change the name of the default Group. *(If you click any other tree icon before saving your changes, AirDefense will prompt you to save them.) Click* **Reset** *to undo unsaved edits.*
4	Click **Commit.**

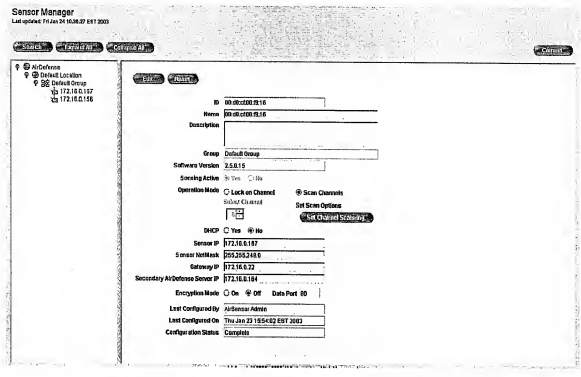


Steps to Edit a Group in AirDefense

Step	Action
1	Click on an existing Group in the Sensor Tree View. *The Edit location screen appears on the right with the name and description of the Location in the Name field.*
2	Click Edit to edit the fields. *(If you click any other tree icon before saving your changes, AirDefense will prompt you to save them.) Click* **Reset** *to undo unsaved edits.*
3	Click **Commit.**

4.2.3 Configuring Sensors

While you initially had to configure each Sensor's network information and mode of operation via a browser using the Sensor's built-in web AirDefense Server, once it connects to the AirDefense Server, you may edit those parameters from Sensor Manager.



Steps to Edit the Sensor Configuration

Step	Action
1	Click on an existing Sensor in the Tree View. *The Sensors screen appears on the right with the ID, Name, and Description of the Sensor you selected.*
2	Click **Edit** to edit the fields (for an explanation of the fields, see the table that follows). *(If you click any other tree icon before saving your changes, AirDefense will prompt you to save them.) Click* **Reset** *to undo unsaved edits.*
3	Click **Commit**.

Steps to Delete a Sensor

Step	Action
1	Click a Sensor in the Tree View, then right click. *The Sensors screen appears on the right of the tree, and a Delete Sensor selector screen appears.*

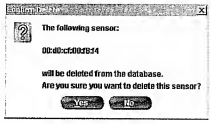
2 Select **Delete Sensor** on the screen.

A Confirm Delete screen appears.

3 Click **Yes** to delete the Sensor from the WLAN.

Alternately, you can click NO to return to the Sensors screen with no changes.

4 Click **Commit** to save your changes.



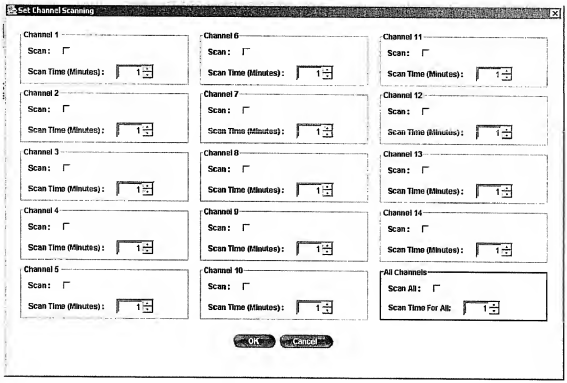
The table below describes each field in each category of the Sensors screen. Some fields are auto-detected. You cannot edit these fields.

Field	Description
ID	Sensor MAC address--auto-detected by AirDefense; cannot be edited.
Name (alias)	User-configured unique name.
Description	User-configured unique description.
Group	Group to which the Sensor belongs---auto-detected by AirDefense; cannot be edited.
Software Version	Version of the Sensor software--auto-detected by AirDefense; cannot be edited.
Sensing Active	This indicates whether or not the Sensor is currently active on the WLAN-auto-detected by AirDefense; cannot be edited.
Operation Mode	Select one of two modes: • **Lock on Channel:** The Sensor listens to network traffic on the selected channel. If you choose Lock on Channel, you must configure the channel. Do this by using the Select Channel picklist. Select Channel 1 *Note:* Although the Sensor is configured to receive data on the selected channel, it may also receive data from adjacent channels, due to the overlapping nature of radio signals.This data also displays in the AirDefense GUI. *Note:* The Sensor's default setting is to lock on channels 1, 6, and 11. • **Scan Channels:** The Sensor will continuously scan one or more channels that you select, 1-14, and spend a length of time you define on each channel before moving to the next. When selected, a Channel Manager button becomes enabled. (Resting your mouse over the Channel Manager button displays a rollover window showing the channels on which the Sensor is currently configured to listen.) Clicking Channel Manager while in Edit mode opens a Java applet window in which you may select channels and the length of time the Sensor should listen on it (see "Channel Manager" on page 73.) Set Scan Options Channel Manager

Field	Description
DHCP	• Yes: Select Yes to use DHCP to assign an IP address to the Sensor • **No:** Select **No** if you choose not to use DHCP to assign an IP address to the Sensor *Note:* You may optionally use DHCP (Dynamic Host Control Protocol) to assign an IP address to the Sensor. If DHCP is disabled, you *must* provide a valid IP address, netmask, and gateway IP address in order for the Sensor to communicate with the AirDefense Server.
Sensor IP	If you selected No to use DHCP, assign a valid IP address to the Sensor.
Sensor NetMask	If you selected No to use DHCP, assign a valid netmask o the Sensor.
Sensor Gateway IP	If you selected No to use DHCP, assign a valid Gateway IP to the Sensor.
Secondary AirDefense Server IP	If you selected **No** to use DHCP, enter an alternate IP address for another AirDefense Server, if you have one in your WLAN. The Sensor can accept more than one IP address. This gives an alternate IP address to the AirDefense Server, in the event that the network path from the Sensor fails. *Note:* This feature applies when more than one AirDefense Server exists in your WLAN. If the connection to the primary AirDefense Server is lost, the Sensor can redirect to a secondary AirDefense Server.
Encryption Mode	• **On:** Choose **On** if you want to encrypt data between the Sensor and the AirDefense Server. This provides additional security. If you choose this option, you must enter a Data Port in the Data Port field. — **Data Port:** If you turn Encryption Mode On, the Sensor defaults to Port **443**. *Note:* To use this option, your AirDefense Server software must be **Release 3.0** or later. • **Off:** Choose **Off** if you do not want to encrypt data between the Sensor and the AirDefense Server. — **Data Port:** If you turn Encryption Mode OFF, the Sensor defaults to Port **80**.
Last Configured By	Auto-detected by AirDefense; cannot be edited. This field reports whether the most recent configuration of the Sensor was made from within the AirDefense GUI, or from within the Sensor UI. If Sensor Admin displays the most recent configuration was made from the Sensor UI; if AirDefense Admin displays, the most recent configuration was made from the AirDefense (Server) GUI.
Last Configured On	Auto-detected by AirDefense; cannot be edited. This field reports the timestamp when the Sensor was last configured.
Configuration Status	Auto-detected by AirDefense; cannot be edited. This field reports the status of the Sensor configurations you last downloaded from the AirDefense Server.The status can be either Pending or Complete. The status remains pending until the Sensor reports back to the AirDefense Server. Normally, this takes about one minute

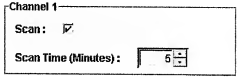
Channel Manager

Clicking on the Channel Manager button opens a Channel Scanning Options screen.



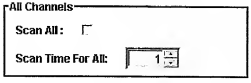
Place a check in the check box for each channel you want AirDefense to scan.

Below each channel check box is a user-input field for setting the number of minutes the Sensor should monitor that channel. Either type a number or use the spinner arrows to create minute values. The Sensor will listen for the specified number of minutes before moving to the next channel.



If only one channel is selected, the Sensor scans it continuously 24 hours a day. If more than one channel is selected, the Sensor first begins scanning the lowest channel (e.g., "1"), then switches to the next highest channel selected, and so on. After scanning the highest selected channel, it returns to the lowest channel again, and repeats throughout the day and night, listening on each channel for the specified number of minutes.

Select the **Scan All** check box to immediately select *all* channels. (Un-check the check box to de-select a channel.)



To quickly apply the same minute value to all channels, enter a number in the input field beside Scan All and click **Set Time For All**.

The results of Sensor channel scanning display in Reports (see Chapter 7, Reports). *Statistics for each channel will only be available for the minutes the Sensor was actually scanning it.*

Adjacent Channel Reception and Sensor Deployment

Because of the nature of radio transmission, a Sensor may receive overlapping signals from adjacent channels, even though you configured the Sensor to lock on a single channel. Some of AirDefense's reports on network traffic will report the data from adjacent channels in addition to the data from the selected channel.

Because radio signals overlap adjacent channels, most WLANs deploy multiple Access Points on channels as widely separated as possible—for example, on channels 1, 6, and 11. This is the default channel setting for AirDefense Sensors.You have two options for deploying AirDefense's Sensors: Dedicate one Sensor to listen to each Access Point, or, use one Sensor to monitor several Access Points. (If using one Sensor to listen to more than one Access Point, you configure it to scan the actual channels your Access Points are broadcasting on. You then define the number of minutes the Sensor scans each channel (i.e., monitor the Access Point's traffic on that channel) before switching to the next channel.

Transmission Channels

There are only eleven transmission channels allowed by law in the U.S. However, since AirDefense does not transmit--it only passively scans--it allows you to scan all 14 channels specified by the 802.11b protocol and configurable in the wireless cards. AirDefense assumes that hackers will not be constrained by the eleven-channel legal restriction.

Click on Search to easily find Locations, Groups, and Sensors.

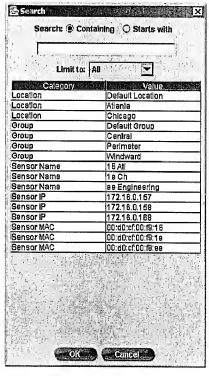
When the number of Locations, Groups, and Sensors is small, it is relatively easy to find them in the left pane of the Sensor Manager window. However, as the number of deployed Sensors increases, it may become time-consuming to scroll through (and expand) numerous Locations and Groups for the Sensor you need to find.

4.3.1 Using Search for Locations, Groups, and Sensors

Follow the steps below to search for Locations, Groups, and Sensors.

Steps to Use Search

Step	Action
1	Click on **Search**.  *The Search window opens.*
2	Choose a search criteria: **Containing** or **Starts with**
3	Enter the Sensor MAC address, IP address, or Name.
4	Choose a search limit: The choices are: • All • Location • Group • Sensor Name • Sensor IP • Sensor MAC
5	Click **OK**. *The search results are based on the search choice you made in step 4.*



Search String

AirDefense looks for an exact match of the search string you enter, and searches are case-insensitive. Therefore, a search for "atlanta" will not find "Atlanta." Neither will a search for "atl" find "atlanta."

5 Policy Manager

Policy Manager enables you to define policies and monitor your WLAN. Use Policy Manager to do the following:

- Create and apply policies for individual and multiple Sensors, Access Points, and Stations in your WLAN.

  Policies are behaviors that you can assign to Sensors, Access Points, and Stations in AirDefense. When AirDefense detects traffic that violates your policies, it generates alarms and alarm reports.

  AirDefense has generic default policies designed for rapid deployment. AirDefense gives you the flexibility to go beyond the default polices by using Policy Manager's configuration editing function to form your own custom policies. Using the Policy Manager, you can create and apply your own alarm-generating policies to Sensors, Access Points, and Stations.

- Pre-configure and add Access Points and Stations into AirDefense, either manually, or by importing via flat file.

  You can import lists of pre-authorized Access Points, Stations, and User Credentials from an ASCII comma delimited flat file.

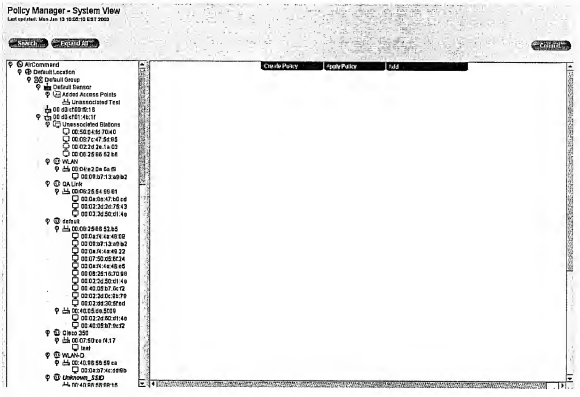
- See views of the historical associations and behaviors of Senors, Access Points, and Stations in your WLAN.

  Using a icon and color-coded Tree View, Policy Manager gives you an historical observed state of the activity that has been taking place in AirDefense. You can use this information to track Access Point-Station associations so that you can better maintain your WLAN.

5.0.1 In This Chapter

This chapter contains the following topics.

The screen below shows the Policy Manager System View. It shows the working screen area on the right, and the Policy Manager Tree View on the left



Policy Manager has two windows, the Policy Manager Tree View on the left, and the working screen on the right. The working screen has pull-downs that reveal more screens.

- To create and apply policies to individual Sensors, Access Points, and Stations, use the Tree View. See "Policy Manager Tree View" on page 79
- To create and apply policies to more than one Sensor, Access Point, and Station, use the pull-down menus. See "Using Policy Manager Screen Pull-Downs" on page 81

5.1.2 Policy Manager Tree View

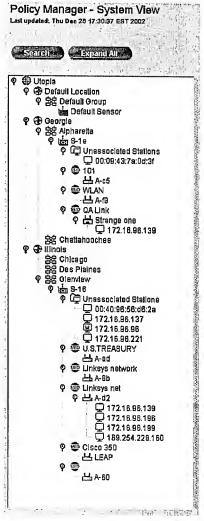
The left-hand window is the Policy Manager Tree View--a hierarchal tree that uses color-coded icons to show the historical Location, Group, Sensor, SSID, Access Point, and Station associations in your WLAN network, and their state since last **Refresh**. The tree gives an historical, not real-time, view of states. It displays regardless of which Policy Manager configuration screen you are currently working in.

Tree View is navigational aide that will help you manage the Sensors, Access Points, and Stations in your WLAN. It is a true, structured hierarchy, with the highest level at AirDefense (system) View and the lowest level at Station View.

Each item in the tree has a color-coded icon that has a specific meaning (see "Color Codes" on page 83).

- **Colors** in Tree View identify the historical state of each network element on the tree (see "Color Codes" on page 83)
- **Icons** in Tree View identify network elements and their historical associations at the System, Location, Group, Sensor, Access Point, and Station levels (see "Icons" on page 86)

  Important: In certain cases, the meanings of icons may differ slightly, depending on if the icon appears in the Tree View, or on one of the many screen tables that appear throughout the GUI. See "Icons" on page 86.



5.1.3 Using Policy Manager Tree View

Steps to Expand or Collapse Tree View

1 Click **Expand All** to expand Tree View.

The entire tree expands to display all Sensors, Access Points, and Stations in your network.

Note: Locations, Groups, Sensors, and Access Points appear only in one place on Tree View. Stations can appear in more than one place on Tree View, matching their associations with Access Points.

2 Click **Collapse All** to close the Tree View.

The entire tree collapses up to the System (your company) icon.

Steps to Update Tree View

You cannot move items around in Tree View. The tree is based on actual observed behaviors in the network. You can, however, delete Access Points and Stations from the tree. The AirDefense Server updates information as it receives new information, but the tree does not reflect these changes automatically. You cannot move items in the tree itself, as the tree is based on actual observed behaviors in the network. To keep track of the Sensor, Access Point, and Station associations in you network, you must manually update the tree.

Step	Action
1	Click on **Refresh** at the top right corner of your screen.

The tree will immediately reflect configuration changes made throughout the entire AirDefense GUI.

Configuring Individual Sensors, Access Points, and Stations

You can use Tree View to create and apply policies for **individual** Sensors, Access Points, and Stations in your WLAN. You can access three screens, which appear to the right of the tree, by clicking on icons directly on Tree View. These are:

- Sensor Policy (see "Sensor Policy" on page 91)
- AP View (see "AP View" on page 94)
- Station View (see "Station View" on page 96)

The table below describes the configuration screens.

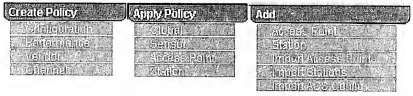
Field	Description
Sensor Policy	Access this field by clicking on a Sensor on Tree View. Use this field to set a Sensor's CRC Errors Threshold and to edit Channel Policies per Sensor.

Field	Description
AP View	Access this field by clicking on an Access Point on Tree View. Use this field to view information about an Access Point. You can also use this field to enter an Access Point's name, designate the Access Point as a bridge, Authorize/Unauthorize/Ignore the Access Point, or edit the Access Point's Configuration, Performance, or Vendor policies.
Station View	Access this field by clicking on a Station on Tree View. Use this field to view Station information, including Access Point associations. You can also use this field to enter a Station name, a Station Description, a Station IP address, place the Station on a Watch List or Ignore List, and Authorize/Unauthorized Stations for Access Points.

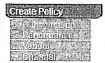
5.1.4 Using Policy Manager Screen Pull-Downs

The Policy Manager screen has pull-downs. Use these to create and apply policies for multiple Access Points and Stations, and to add Access Points and Stations to your WLAN.The pull-downs are:

- Create Policy
- Apply Policy
- Add



The table below describes the pull-downs

Field	Description
Create Policy	Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to create configuration, performance, vendor, and channel policies for your Sensors, Access Points, and Stations The screens are: • Configuration • Performance • Vendor • Channel fields 

Field	Description
Apply Policy	Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to apply Global, Access Point, Sensor, and Station policies to your Access Points, Sensors, and Stations.The screens are: • Global • Sensor • Access Point • Station 
Add	Access this set of AirDefense fields from the main Policy Manager screen. Use these fields to pre-configure (including authorization) and add Access Points or Stations to your network, import Access Points or Stations from another location, and add ACS Configurations to your WLAN. The screens are: • Access Point • Station • Import Access Points • Import Stations • Add ACS Configuration. 

5.1.5 Color Codes

Each icon that appears in Policy Manager in either the Tree View or the GUI screens has a color that represents a state.

- Individual Access Points and Sensors display in a single color that represents their current state.
- A single Station can display in two or more colors, depending on its configuration in relationship to its Access Point.

Important: In certain cases, the meanings of icons may differ slightly, depending on if the icon appears in the Tree View, or on one of the many screen tables that appear throughout the GUI.

The table below lists the colors and their meanings.

Color	Meaning
Blue	Blue indicates a default placeholder state for Sensors, Access Points, or Stations that are not observed by AirDefense. Placeholder items are always a manually-added or an imported Access Point or Station. ***They will always be Blue.*** ***Note:*** When you import an Access Point that has never been entered into AirDefense, it will be Blue, even if you authorized in its configuration in the import file. When AirDefense detects the newly imported Access Point, the state changes to either authorized (Green) or unauthorized (Red), depending on your configuration in the import file.
Grey	Grey indicates that a Access Point or Station is being ignored by the AirDefense Server. For more information on Ignore, see Chapter 5, Policy Manager. ***Note:*** AirDefense sees devices that are in the ignored state, but does not generate an alarm unless an attack occurs.

Color	Meaning
Red	Red indicates the following: • **Sensor:** Offline, which indicates that the Sensor is not communicating with the AirDefense Server for one of the following reasons: — Sensor has been observed by the Server, but is currently not connected to the Server. — Sensor is connected to the Server, but is configured for **Active: no** operation (see "Configuring Sensors" on page 19). *Note:* If you did not intentionally take a Sensor offline, perform appropriate steps to reboot the Sensor (see Chapter 1, Installation & Log In). • Access **Point:** Unauthorized — All Access Points are unauthorized when they are first discovered by AirDefense. They remain unauthorized until an administrator changes their state to authorized. If you manually add or import an Access Point, you can configure it as authorized at that time, in which case, it enters AirDefense as Blue. • **Station:** Unauthorized on a given Access Point — Unauthorized indicates that the Station is not authorized for the Access Point it appears under — The same Station can appear as Red or Green, depending on whether or not they are authorized on the Access Point they are under — Stations have a W on Green or Red if they are on the user-configurable Watch List (for more information on the Watch List, see Chapter 5, Policy Manager). *Note:* AirDefense generates an alarm once per minute, per device, as long as the device remains unauthorized.
Green	• Stations — Station is authorized under the Access Point and has been observed as associated to that Access Point • Access Points — Access Point is authorized and has been observed by a Sensor • Sensor — Green indicates that the Sensor is functioning normally and in communication with the AirDefense Server.To be in this state, the following is required: >>The Sensor must be connected to the Server--the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). >>The Sensor must be configured for **Active: yes** operation (see "Configuring Sensors" on page 19).

Color	Meaning
Purple	Purple can have two meanings: • In all GUI program areas with the exception of Policy Manager, Purple indicates that the Station has been observed, but not currently associated, with any Access Point at that time. • In Policy Manager, Purple indicates that a Station has never been associated with an Access Point.
Orange	Orange indicates Ad Hoc activity. There are two Orange icons: • Ad hoc Network • Ad hoc Station

5.1.6 Icons

Each network element in the AirDefense WLAN is represented by an icon. Icons can either represent a physical device, such as an Access Point, Station, or Sensor, or logical associations, such as an SSID, a Location, or a Group.

The tables below list the icons and their meaning

Magnifying Glass

Icon	Color/State	Meaning
	Static	Magnifying Glass. This icon can appear on all items in the Tree View with the exception of the Station. It indicates that the item is expandable or collapsible. Clicking on the icon next to a tree item expands that item; clicking again, collapses the item. For example, clicking on the magnifying glass next to an Access Point reveals the Stations that have associated with that Access Point.

AirDefense (System) Icon

Icon	Color/State	Meaning
	Static	This is the highest level in the tree, representing the AirDefense Server.

Location Icon

Icon	Color/State	Meaning
	Static	This is the second highest level in the tree, representing the Sensor Location. Expand the Locations to expose the individual Groups for a particular Location.

Group Icon

Icon	Color/State	Meaning
	Static	This is the third highest level in the tree, representing the Sensor Group. Expand the Groups to expose the individual Sensors for a particular Group.

Sensor Icons

Sensors can be three different colors, representing three states. These are Blue, Red, and Green. Sensor icons can also have a CH or SC on the icon. The CH indicates that the Sensor is configured for Channel Lock; the SC indicates that the Sensor is configured for Scan Channels (see "Configuring Sensors" on page 70 for more information on these configurations). .

Icon	Color/State	Meaning
	Blue: Not observed by the AirDefense Server; not online or active	Default Sensor The Default Sensor is a placeholder, not a real online Sensor. This is a place to put Stations and Access Points that you have manually added or imported, and authorized into AirDefense. AirDefense has not yet physically observed these. ***Note:*** Access Points entered into AirDefense always appear as blue, and always at the top of the tree under Default Sensor until they are seen by AirDefense. Once observed, they become green, red, or grey, and are moved out of the list, but not automatically. You must click **Refresh**.
	Green: Online **CH**=Channel Lock **SC**=Channel Scan	Online Sensor Sensor is functioning normally and is communicating with the AirDefense Server.To be in this state, the following are required: • The Sensor must be connected to the Server--the Sensor IP address must match the Server IP address (see "Configuring Sensors" on page 19). • The Sensor must be configured for **Active:** yes operation (see "Configuring Sensors" on page 19).
	Red: Offline **CH**=Channel Lock **SC**=Channel Scan	Offline Sensor Sensor is not communicating with the AirDefense Server for one of the following reasons: • Sensor has been observed by the Server, but is currently not connected to the Server. • Sensor is connected to the Server, but is configured for **Active: no** operation (see "Configuring Sensors" on page 19).

SSID Icon

Icon	Color/State	Meaning
	Static	SSID This is the logical group to which the Access Points belong.

Access Point Icons

Access Points and Bridged Access Points can be four different colors, representing four states. These are Blue, Red, Green, and Grey.

Icon	Color/State	Meaning
	Blue: Unobserved	Unobserved Access Point Access Points that are blue are not yet seen by a Sensor.
	Blue: Added Access Point Folder	Added Access Point Folder This folder contains Access Points that have been added manually or imported, but have not yet been seen by a Sensor.
	Green: Authorized	Authorized Access Point ***Note:*** Access Points that you enter manually or import are appear as blue, and always at the top of the tree under Default Sensor. Once they are seen by AirDefense, they are moved out of the list, but not automatically. You must click **Refresh.**
	Red: Unauthorized	Unauthorized Access Point On discovery, all Access Points come into AirDefense unauthorized. ***Note:*** An exception to this is if you previously added or imported the Access Point, at which time you can choose to authorize the Access Point. When it is seen by AirDefense, the Access Point will change from blue to green and move under the discovering Sensor.
	Grey: Ignored	Ignored Access Point Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates alarms. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.
   	Blue: Unobserved Green: Authorized Red: Unauthorized Grey: Ignored	Bridged Access Point ***Note:*** Bridges are user-defined for informational purposes. Two or more Access Points can serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired Access Point. For more information, see Appendix D on page 259.

Station Icons

Stations can be five different colors, representing five states. These are Purple, Green, Red, Grey, and Orange.

- Green and Red Stations can have a "W" on the icon, indicating they are on the Watch List.
- A Station can appear as Green, Red, or Grey under different Access Points, depending on the configuration.

Icon	Color/State	Meaning
	Purple: Unassociated Purple with "W": Authorized, and on Watch List	Unassociated Station Purple Stations have two meanings: • In all GUI program areas with the exception of Policy Manager, a Purple Station indicates that the Station has been observed, but not currently associated with any Access Point at that time. • In Policy Manager, a Purple Station indicates that the Station has never been associated with an Access Point. It always appears under the Unassociated Stations folder in Policy Manager.
	Green: Authorized Green with W: Authorized, and on Watch List	Authorized Station This is a Station that is authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List. ***Note:*** An authorized Station may appear as Unauthorized (Red) or Ignored (Grey) under a different Access Point.
	Red: Unauthorized. Red with W: Unauthorized, and on Watch List	Unauthorized Station This is a Station that is not authorized on the Access Point it appears under. A W indicates that the Station is on the Watch List. Unauthorized Stations generate alarms once per minute, per MAC address, for as long as the AirDefense Server recognizes the Station. ***Note:*** An unauthorized Station may appear as Authorized (Green) or Ignored (Grey) under a different Access Point.
	Grey: Ignored	There are two types of Grey Stations: • Station is configured for Ignore--*not alarm generating* — All activity by this Station is ignored by AirDefense. It does not generate alarms in AirDefense, regardless of activity. • Access Point is configured for Ignore--*alarm generating.* — If you configure an Access Point as Ignored, any Station under the Access Point also become Ignored in terms of traffic on that Access Point. If the Station starts doing anything outside of configured policies, AirDefense generates alarms.

Icon	Color/State	Meaning
	Orange: Ad Hoc:	Ad Hoc Station An ad hocStation is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc networks and reports the network's Device Identifiers and other information.
	Grey folder/Blue Station: Unassociated	Unassociated Stations The Unassociated Station folder contains Stations in a manual state that are observed by the AirDefense, but that have never been associated with an Access Point. Stations under this folder appear as Purple.

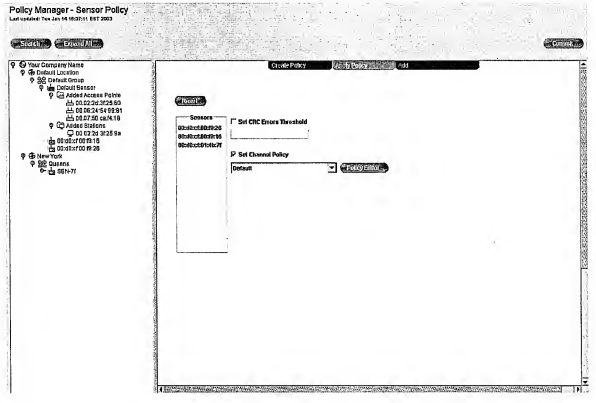
Ad Hoc Network Icon

Icon	Color/State	Meaning
	Orange: Ad Hoc	Ad Hoc Network An ad hoc network is a User Station that is connected to one or more other User Stations without using an Access Point. It does not need a wireless infrastructure, and therefore represents a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. AirDefense detects ad hoc networks and reports the network's Device Identifiers and other information. ***Note:*** The software that controls the functionality of wireless network adapters typically provides the ability, configured manually, to accomplish ad hoc networking.The software creates a session ID—much like the MAC address of an Access Point—which the devices use to communicate with each other.

Use the **Sensor Policy** screen to configure CRC Errors Thresholds and Channel Policies for individual Sensors.

You can navigate to this screen by:

- Clicking on any individual Sensor in Tree View.



Steps to Use Sensor Policy

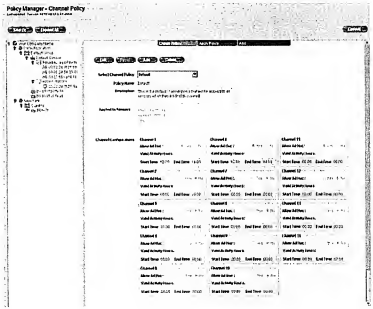
Step	Action
1	Click **Expand All** to expand Tree View and reveal the individual Sensors in the WLAN.
2	Click on any Sensor in Tree View to configure policies for an individual Sensor. *The Sensor Policy screen appears.*
3	Configure CRC Errors Thresholds and Channel Policies for the individual Sensor. You must check the boxes to activate the fields.
4	Click **Commit.**
5	Alternately, you can click **Reset** to clear changes.

The table below lists the fields in Sensor Policy.

Field	Purpose
Sensor ID	Device identifier of the Sensor.
Sensor Name	User-Configured Name of the Sensor. You designate the name of the Sensor when you configure the Sensor (see "Configuring Locations, Groups, and Sensors" on page 67). **Example:** *Floor One South.*
CRC Errors Threshold	This is the threshold for the number of CRC (transmission) errors allowed in the WLAN the Sensor is monitoring. Enter a number of CRC errors per minute each Sensor may detect as it listens to the traffic in its reception area. High numbers of CRC errors may indicate that two or more Access Points are sharing the same channel; colliding with each other; that an object is interfering with the signal; or that a hacker may be flooding your air space with bad data in a Denial of Service attempt. *Note:* Unusually high numbers of CRC errors indicate network performance problems or the activity of a hacker.

Field	Purpose
Channel Policy	The pick list displays all saved channel policies. Select a channel policy from this list to apply to the Sensor. ***Default policies cannot be edited.***

Note: Alternately, you can click Policy Editor to go to the Channel Policy Editor screen and edit, add, or delete channel policies for the Sensor (see "Create Policy: Channel" on page 112).



- **Channel Number:** You must make configurations for each of the 14 channels.
- **Allow Ad Hoc:** Choose **Yes** to allow Ad Hoc; **No** to disallow Ad Hoc. Ad Hoc is independent of activity hours

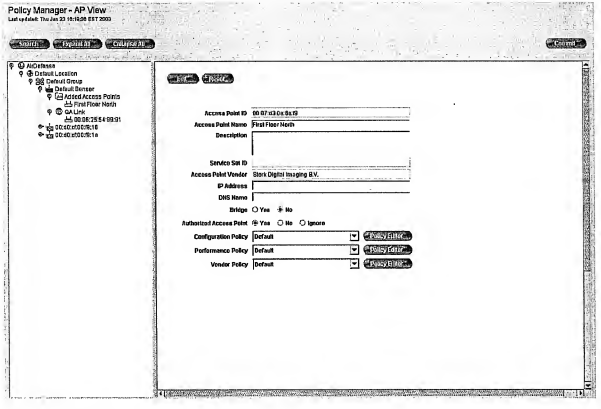
  Note: An ad hoc station is a User Station that is connected to one or more other User Stations without using an Access Point. Ad hoc networking is a function of most standard 802.11 network client cards. User Stations that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network.
- .**Valid Activity Hours:** For each channel, enter a **Start Time** and **End Time** in the input fields.

  Note: Enter times in a 24-hour format, using the format HH:MM. Traffic is *only* allowed between the start and end hours. Traffic detected on the channel outside the valid activity hours generates an alarm.

Use the **AP View** screen to configure individual Access Points in your WLAN.

You can navigate to this screen by:

- Clicking on any individual Access Point in **Tree View.**



Steps to Use AP View

Step	Action
1	Expand Tree View reveals the individual Access Points in the WLAN.
2	Click on any Access Point in Tree View to configure policies for an individual Access Point. *The AP View screen appears.*
3	Configure the fields in the screen.
4	Click **Commit.**
5	Alternately, you can click **Reset** to clear changes.

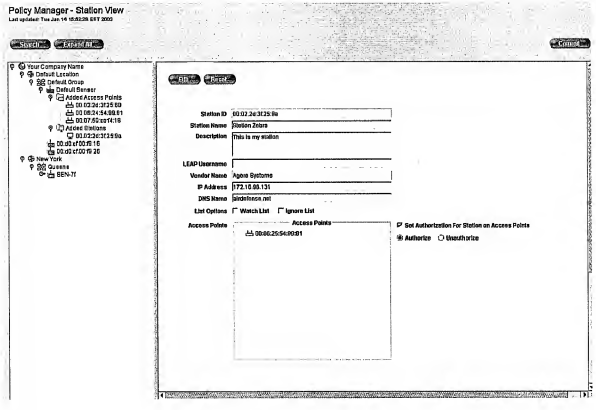
The table below lists the fields.

Field	Purpose
Access Point ID	Device Identifier of the Access Point. This is a required field.
Name	Name of the Access Point (optional). If you chose a name for the Access Point, it appears here.
Description	A description of the Access Point (optional)
Service Set ID	SSID number (this is not the same as the Access Point ID).
Access Point Vendor	Equipment manufacturer of the Access Point. This is automatically pulled by AirDefense.
IP Address	The IP address of the Access Point.
DNS Name	The Access Point's DNS Name assignment (if applicable).
Bridge	• **Yes:** Click Yes if you are using this Access Point as a Bridge • **No:** Click No if you are not using this Access Point as a Bridge ***Note:*** A Bridge is two or more Access Points that serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired AP (see Appendix D: Glossary).
Authorized Access Point	• **Yes:** Click **Yes** to authorize this Access Point for use in your WLAN • **No:** Click **No** to unauthorize this Access Point for use in your WLAN • **Ignore:** Click **Ignore** to place this Access Point in an Ignored state. ***Note:*** Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates an alarm. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.
Configuration Policy	Leave the default configuration policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Configuration Policy Editor screen if you wish to edit, add, or delete configuration policies. 
Performance Policy	Leave the default performance policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Performance Policy Editor screen if you wish to edit, add, or delete performance policies. 
Vendor Policy	Leave the default vendor policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Vendor Policy Editor screen if you wish to edit, add, or delete vendor policies.

Use the **Station View** screen to configure individual Stations in your WLAN.

You can navigate to this screen by:

- Clicking on any individual Station in Tree View.



Steps to Use Station View

Step	Action
1	Expand Tree View reveals the individual Stations in the WLAN.
2	Click on any Station in Tree View to configure policies for an individual Station. *The Station View screen appears.*
3	Configure the fields in the screen.
4	Click **Commit**.
5	Alternately, you can click **Reset** to clear changes.

The table below describes the fields in Station View.

Field	Purpose
Station ID	MAC address of the Station. AirDefense automatically generates this field. *Note:* You enter the Station ID when you add the Station to the WLAN (see "Add: Station" on page 126)
Name	User-configured name of the Station (optional). *Note:* You can choose to give the Station a unique name, no longer than 15 characters, when you add the Station to the WLAN (see "Add: Station" on page 126).
Description	A description of the Station (optional). *Note:* You can choose to give the Station a description when you add the Station to the WLAN (see "Add: Station" on page 126).
LEAP Username	This field applies if you are using EAP Configuration Mode in your configuration policy definition. (See "Create Policy: Configuration" on page 99.)
Vendor Name	Equipment manufacturer of the Station. AirDefense automatically generates this field.
IP Address	The IP address of the Station. This field displays an IP address if you chose to enter an IP address when you added the Station to the WLAN (see "Add: Station" on page 126).
DNS Name	The Station's DNS Name assignment (if applicable).
List Options	If you are going to use a List Option, the option must be either Watch List, or Ignore. • **Watch List:** Click on this checkbox if you wish to know if this Station's MAC address will occur in your network again. The next time the AirDefense Server sees this Station, it will generate an alarm for every minute the it sees this Station's in the network. • **Ignore List:** Click on this checkbox if you wish the AirDefense Server to ignore the presence of a Station on the network. AirDefense does not generate an alarm for any MAC address on the Ignore list. *Note:* This feature is useful if you want to keep certain unauthorized Stations that your AirDefense Server sees from alarming, as in the case of Stations in an adjacent office that belong to another Company. Placing these known "friendly" Stations on the Ignore list prevents continuous false alarms.

Field	Purpose
Access Points	List of Access Points that the Station is associated with on your WLAN. AirDefense pulls this list.
Set Authorization For Station on Access Points	• You must click on the checkbox before selecting authorize/unauthorize. • **Authorize:** Select **Authorize** if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. • **Unauthorize:** Select **Unauthorize** if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations *not authorized* are assumed to belong to hackers or violators of your wireless network policy.)

To create policies, you must access four screens. These are:

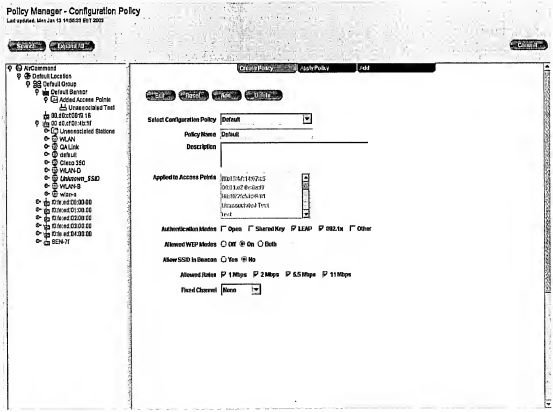
- Configuration
- Performance
- Vendor
- Channel

5.5.1 Create Policy: Configuration

Use the **Create Policy: Configuration** screen to create and edit configuration policies for multiple Access Points in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Configuration**
- Clicking on any Access Point in **Tree View**, and then clicking **Configuration Policy: Policy Editor**. 
- Clicking on **Apply Policy: Access Point**
- Clicking on **Ad Policy: Access Point**



Steps to Use Create Policy: Configuration

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Create Policy: Configuration** *The Configuration Policy screen appears.*
3	To edit the fields, click on **Edit.** *You can click **Reset** at any time to get out of Edit mode without saving your changes.*
4	To add a configuration policy to the database, click **Add** (Add is disabled while in Edit mode).
5	To permanently remove a configuration policy from the database, click **Delete** (Delete is disabled while in Edit mode).
6	Click **Commit.**

The table below describes the fields in the **Create Policy: Configuration** screen.

Field	Purpose
Select Configuration Policy	Select the configuration policy from the pull-down. *Note:* You cannot configure a default policy.
Policy Name	Enter the name of the policy in this field.
Description	Enter a description of the policy in this field.
Applied to Access Points	You cannot edit this field. This field shows the Access Points that your policy applies to. It lists the device identifiers of all Access Points detected by AirDefense in the last thirty days.

Field	Purpose
Authentication Modes	Choose a mode to configure the Access Point to accept non-authenticated network connections, and/or shared key authentication. AirDefense generate alarms if it detects that the Access Point is allowing Stations to associate with it using a method not allowed here. • **Open:** This type of authentication allows any Station to associate with it—*the equivalent of no authentication.* • **Shared Key:** This type of authentication requires an encrypted key authentication before the Access Point allows Stations to associate with it. Key-sharing exposes the key to hackers. You may want to use an alternate authentication method--*Other.* • **LEAP:** EAP Authentication Mode--This option gives AirDefense the ability to detect LEAP authentication. You can set Access Point configuration policies to require LEAP authentication. Failure of the Access Point to operate contrary to this policy generates an alarm. Using this in your policy definition ensures that LEAP is deployed and being used by both Access Points and Stations. If an Access Point or Station is misconfigured and not running LEAP, AirDefense generates an alarm for either instance. • **802.1x:** EAP Authentication Mode--This option gives AirDefense the ability to detect 802.1x authentication. You can set Access Point configuration policies to require 802.1x authentication. Failure of the Access Point to operate contrary to this policy generates an alarm. Using this in your policy definition ensures that 802.1x is deployed and being used by both Access Points and Stations. If an Access Point or Station is misconfigured and not running 802.1x, AirDefense generates an alarm for either instance. • **Other:** An alternate means of your choosing.
Allowed WEP Modes	As a minimal security measure, you should enable Wired Equivalent Privacy (WEP) on every Access Point • **On:** Enables WEP for the Access Point • **Off:** Disables WEP for the Access Point • **Both:** Allows either On or OFF, and does not generate an alarm for either. ***Note:*** Set the WEP policy to **On** and the Access Point to **Off** to enable alarms. If AirDefense detects the Access Point using WEP differently than specified here, it generates an alarm.
Allowed SSID in Beacon	SSID (Service Set IDs) are not passwords. They are broadcast in a beacon. • **Yes:** Access Point broadcasts SSID • **No:** Access Point does not broadcast SSID ***Note:*** By default, many Access Points are configured to broadcast their Service Set ID (SSID) within their beacons. ***Note:*** Set the SSID policy to **No** and the Access Point to Broadcast to enable alarms. If AirDefense detects that the Access Point beacon differs from what is specified here, it generates an alarm.

Field	Purpose
Allowed Rates	Each Access Point is configured to transmit and receive data at specified rates. Select the transfer rates you want the Access Point to use. • **1.0 Mbs** • **2.0 Mbs** • **5.5 Mbs** • **11 Mbs** If AirDefense detects the Access Point transmitting or receiving data at a rate not specified here, it generates an alarm.
Fixed Channel	If you want the Access Point to transmit on a fixed channel, you can specify the channel it uses from the pull-down channel list. • **None** • **1-14** If AirDefense detects the Access Point transmitting or receiving data on a different channel than indicated here, it generates an alarm.

5.5.2 Create Policy: Performance

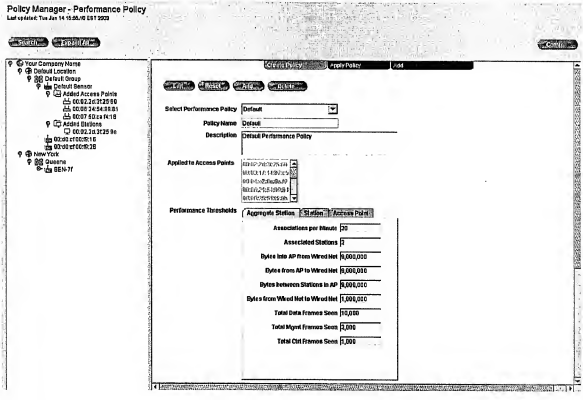
Use the **Create Policy: Performance** screen to create and edit policies for network performance. These consist of a main screen, and three subscreens for configuring Performance Thresholds.

> ***Note:*** AirDefense, Inc. recommends that you monitor network traffic for as long as several weeks, to determine normal network throughput before setting threshold values.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Performance**
- Clicking on any Access Point in Tree View, and then clicking on **Performance Policy: Policy Editor.**

- Clicking on **Apply Policy: Access Point**
- Clicking on **Add: Access Point**

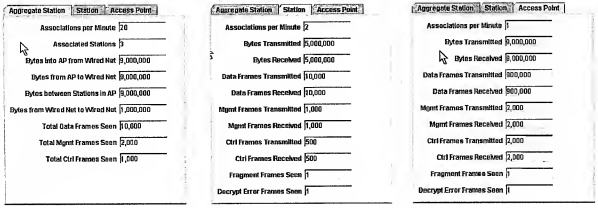


Steps to Use Create Policy: Performance

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Create Policy: Performance**

The Performance field appears.

Three sets of Performance Thresholds occupy the main body of the Create Policy: Performance field: These represent aggregate Station thresholds, individual Station thresholds, and Access Point thresholds. You can navigate through these subfields by clicking on the named folder tabs.



3 To edit the Description and various Performance Thresholds, click **Edit**.

*You can click **Reset** at any time to get out of Edit mode without saving your changes.*

Note: When entering numerical values in the fields: If you want a single digit in the field, select the text and enter the value. You cannot backspace over the last digit in the field.

4 To add a performance policy to the database, click **Add** (Add is disabled while in Edit mode).

5 To permanently remove a performance policy from the database, click **Delete** (Delete is disabled while in Edit mode).

6 Click **Commit**.

The table below lists the top fields in the in the **Create Policy: Performance** screen.

Field	Purpose
Select Performance Policy	This pick list displays all saved policies. Select a policy from this list to edit or delete it. Included in the list is a Default policy (cannot be edited). Newly-discovered Access Points are assigned this policy.
Policy Name	This displays the name of the policy.
Description	This displays a description of the policy.
Applied to Access Points	This memo field displays all Access Points currently configured to use the currently selected policy.

About Thresholds

AirDefense generates alarms if it detects network traffic that exceeds the thresholds you enter in the Performance Thresholds fields. For each Access Point or Station triggering an alarm, AirDefense generates the alarm once per minute for every minute the condition exists.This allows you to detect whenever WLAN traffic exceeds normal limits, and allows you to perform network capacity planning—identifying when and where the WLAN needs to be augmented. You can monitor network traffic on a per-user basis, allowing you to identify which users are consuming the most bandwidth.

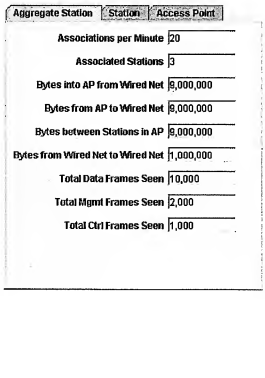
Initially, administrators should set global unauthorized station alarm policies to **Disable** after authorizing all Access Points for the first time.They will then create a *no alarm* Access Point policy and set all default thresholds to **zero**. This is to prevent AirDefense from filling with alarms during the initial deployment. Thresholds can be raised after successful deployment of AirDefense. For complete instructions on this process, see the *Quick Start* guide that came with AirDefense (AD-QS-1.01).

Aggregate Station Thresholds

Aggregate Station Thresholds are the *combined* network characteristics for all Stations and traffic in the Access Point's Basic Service Set (BSS)—i.e., the *footprint* of the Access Point and the Stations associating with it.

Note: Entering a zero value as a threshold anywhere within **Create Policy: Performance** disables alarm-generation for that threshold.

Example: *For example, if the Associations Per Minute threshold for Aggregate Stations is zero, AirDefense will not generate an alarm—even if 5,000 associations are made within one minute.*



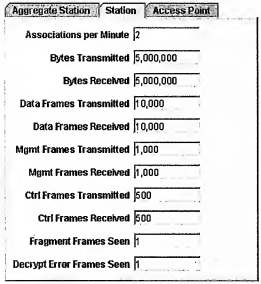
The table below lists the field values in the Aggregate Station table.

Values	Description
Associations per Minute	Enter the maximum number of associations *per minute* AirDefense will allow between the Access Point and all Stations combined. ***Note:*** On the one hand, this number should be low—for example, $\frac{1}{20}$ the number of total Stations in the WLAN. Your Stations should associate with an Access Point once in the morning when employees log on at the beginning of the workday, and rarely after that. On the other hand, if the threshold value represents the actual number of Stations in the BSS, a useful alarm will be generated if the Access Point goes offline, forcing the Stations to re-associate with it. In no case should this value be greater than the actual number of Stations in the BSS. ***Note:*** If the signal strength between the Station and the Access Point is very low, the Station may repeatedly lose connectivity and then reconnect, increasing the number of associations per minute.
Associated Stations (Concurrently)	Enter the maximum number of Stations allowed to associate *at any one time* with this Access Point. This number should reflect your actual number of Stations. If AirDefense detects a greater number, an alarm is generated, assuming that the extra associations are made by hackers.
The values for all the thresholds immediately below should be based upon your "site survey"—what you learned was "normal" for your WLAN. ***Note:*** Take special care when creating the "byte thresholds" that immediately follow. Several factors govern the values you enter for each. • The transmission rate of the Access Point—how much data it can transmit—is the first consideration. If the transmission rate is only 1 megabit per second, the thresholds should be much lower than if the transmission rate is 11 megabits per second. • All four directions of traffic (wired to wired, wired to wireless, wireless to wired, and wireless to wireless) must add up to 100% or less of available bandwidth. Many administrators prefer to set the individual thresholds such that their combined value is 80% or less than available bandwidth. • When setting thresholds designed for capacity planning, the threshold (for all data combined) should be approximately 50% of available bandwidth—that is, 30 MB per minute for an 11 MB transfer rate, and 3 MB per minute for a 1 MB transfer rate.	
Bytes into Access Point from Wired Net	Enter the maximum number of bytes of data per minute allowed into the BSS from the wired portion of your network. If AirDefense detects a greater number, it generates an alarm.
Bytes from Access Point to Wired Net	Enter the maximum number of bytes of data per minute allowed out of the BSS to a wired portion of your network. If AirDefense detects a greater number, it generates an alarm.
Bytes between Stations in BSS	Enter the maximum number of bytes of data per minute allowed to be transmitted within the BSS from all Stations. If AirDefense detects a greater number, it generates an alarm.
Bytes from Wired Net to Wired Net	Enter the maximum number of bytes of data per minute allowed to be transmitted from a wired portion of the network to another wired portion of the network, using the Access Point as a bridge. If AirDefense detects a greater number, it generates an alarm.

Values	Description
Total Data Frames Seen	Enter the maximum number of data frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm.
Total Mgmt Frames Seen	Enter the maximum number of management frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm.
Total Ctrl Frames Seen	Enter the maximum number of control frames per minute allowed to be transmitted from all Stations combined. If AirDefense detects a greater number, it generates an alarm.

Individual Station Thresholds

This set of thresholds apply to any *individual* Station in the Access Point's Basic Service Set, and will typically be lower than the Aggregate Station thresholds. That is, if any *single* Station reaches one of these thresholds, an alarm will be generated. These threshold alarms will tell you *who* the high bandwidth users are, and *when* they are using it. Entering a value of "0" (zero) for any threshold-type disables that specific alarm.

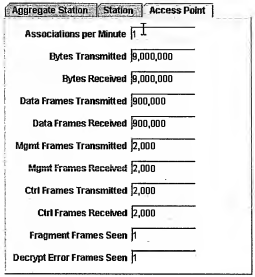


Column	Description
Associations per Minute	Enter the maximum number of associations per minute any Station is allowed to make with an Access Point. On the assumption that most Stations should only associate once when the user logs onto to the network at the start of each work day, and rarely re-associate after that, this number should be low—1 or 2. If AirDefense detects a greater number, it generates an alarm.
The thresholds below should either be based on the "normal" transmission rate that you detected during your initial "site survey," or on arbitrary numbers designed to detect your high-bandwidth users. If you want to be notified, for example, of users who transmit files greater than 10 MB set the "Bytes Transmitted" and "Bytes Received" values to 10,000. If you don't care if users send large files, then set these values to zero (indicating that an alarm for that threshold will not be generated).	

Column	Description
Bytes Transmitted	Enter the maximum number of bytes of data per minute any Station is allowed transmit. If AirDefense detects a greater number, it generates an alarm.
Bytes Received	Enter the maximum number of bytes of data per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Data Frames Transmitted	Enter the maximum number of data frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Data Frames Received	Enter the maximum number of data frames per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Mgmt Frames Transmitted	Enter the maximum number of management frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm. Management frames carry information related to negotiating network connections. If many more Management frames per minute than usual are detected, this could indicate a Denial of Service attack, or that a hacker is flooding the air with "disassociate" or "de-authenticate" commands.
Mgmt Frames Received	Enter the maximum number of management frames per minute any Station is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Ctrl Frames Transmitted	Enter the maximum number of control frames per minute any Station is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Ctrl Frames Received	Enter the maximum number of control frames per minute any Station is allowed to receive. If AirDefense detects a greater number, an alarm is generated. Control frames carry information about negotiating the 802.11 protocol for getting data onto the airwaves, and are transmitted at only 1 Mbs. Unusually high numbers of Control frames may indicate bandwidth and network problems.
Fragment Frames Seen	Enter the maximum number of fragment frames per minute from any Station that are allowed. If AirDefense detects a greater number, it generates an alarm.
Decrypt Error Frames Seen	Enter the maximum number of decrypt error frames per minute from any Station that are allowed. If AirDefense detects a greater number, it generates an alarm.

Access Point Thresholds

This set of thresholds applies to the Access Points themselves, and will typically be less than the Aggregate Station thresholds. These values should all be based on the "normal" WLAN traffic discovered your initial site survey. Entering a value of "0" (zero) for any threshold-type disables that specific alarm.



Column	Description
Associations per Minute	Ordinarily, Access Points do not associate with anyone. However, when an Access Point is used as a "bridge" between two other parts of the wireless network, they must associate with the Access Points with whom they are bridging. Therefore this number should be "1" or the actual number of bridges in use. (If no bridges are deployed, this value should still be "1" as a zero value will disable alarm-generation for this threshold.)
Bytes Transmitted	Enter the maximum number of bytes of data per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Bytes Received	Enter the maximum number of bytes of data per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Data Frames Transmitted	Enter the maximum number of data frames per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Data Frames Received	Enter the maximum number of data frames per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Mgmt Frames Transmitted	Enter the maximum number of management frames per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Mgmt Frames Received	Enter the maximum number of management frames per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm.

Column	Description
Ctrl Frames Transmitted	Enter the maximum number of control frames per minute this Access Point is allowed to transmit. If AirDefense detects a greater number, it generates an alarm.
Ctrl Frames Received	Enter the maximum number of control frames per minute this Access Point is allowed to receive. If AirDefense detects a greater number, it generates an alarm.
Fragment Frames Seen	Enter the maximum number of fragment frames per minute this Access Point may see before generating an alarm.
Decrypt Error Frames Seen	Enter the maximum number of decrypt error frames per minute this Access Point may see before generating an alarm.

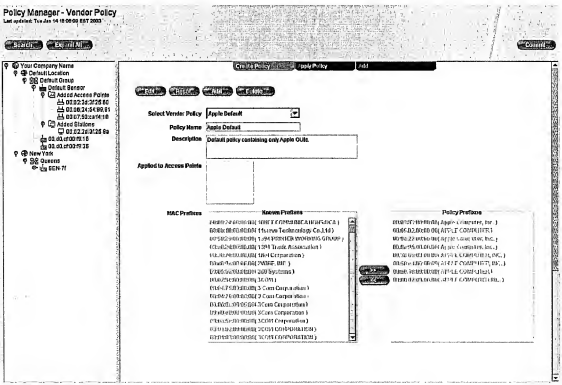
5.5.3 Create Policy: Vendor

Use the **Create Policy: Vendor** fields to ensure that only approved vendor equipment for Access Points and Stations are deployed in your WLAN. Any equipment not on your custom approved vendor list generates an alarm.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Vendor**
- Clicking on any Access Point in Tree View, and then clicking on **Vendor Policy: Policy Editor.**

- Clicking on **Apply Policy: Access Point**
- Clicking on **Add: Access Point**



Steps to Use Create Policy: Vendor

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Create Policy: Vendor** *The Performance field appears.*
3	To edit an existing vendor policy, click **Edit.** *You can click **Reset** at any time to get out of Edit mode without saving your changes.*
4	To add a custom vendor policy to the database, click **Add** (Add is disabled while in Edit mode). *A **Select Policies as Templates** screen appears.* *You can click **Reset** at any time to get out of Add mode without saving your changes.*
5	Select the default vendor you would like to form your custom vendor policy. *A list of all known IEEE MAC prefixes for existing vendor equipment appears in the known prefixes field.* *In the Policy Prefixes field, a list of existing prefixes appears. These are the prefixes that belong to the default vendor you selected.*
6	Use the right and left arrows to transfer prefixes back and forth between screens to form your custom vendor policy.
7	To permanently remove a performance policy from the database, click **Delete** (Delete is disabled while in Edit mode).
8	Click **Commit** to save your input.

The table below lists the fields in the **Create Policy: Vendor** screen.

Column	Description
Select Vendor Policy	This pick list displays all saved vendor policies. Once you formulate a custom vendor policy, it will appear on this list. You can select a policy from this list to edit or delete it. Included in the list is are Default policies---*you cannot edit these.* *Note:* Default vendor policies are predefined and cannot be edited. Create a new vendor policy by using a default policy as a template.
Policy Name	This displays the name of the policy.
Description	This displays a description of the policy.
Applied to Access Points	This memo field displays all Access Points currently configured to use the currently selected policy.
MAC Prefixes	• **Known Prefixes:** These are a list of all of the known IEEE MAC prefixes. • **Policy Prefixes:** These are list of the IEEE MAC prefixes that are vendor defaults, or the prefixes you assign in your custom vendor policy.

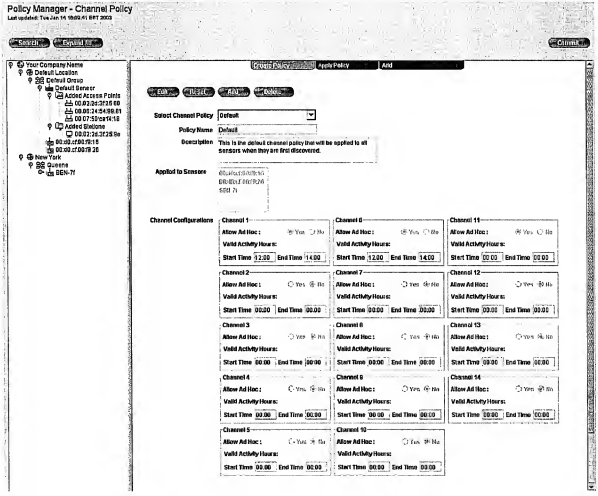
5.5.4 Create Policy: Channel

Use the **Create Policy: Channel** fields to create channel policies for the Sensors in your WLAN. AirDefense allows you to set ad hoc networking and time-of-day policies for individual channels. Whenever one of AirDefense's Sensors detects an ad hoc network or network traffic outside of allowed hours, it generates an alarm.

You can navigate to this screen by:

- Using the screen pull-down **Create Policy: Channel**
- Clicking on any Sensor in **Tree View**, and then clicking on **Channel Policy: Policy Editor.**

- Clicking on **Apply Policy: Sensor** (with **Set Channel Policy** selected)



Steps to Use Create Policy: Channel

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Create Policy: Channel** *The Channel field appears.*
3	To edit an existing channel policy, click **Edit**. *You can click **Reset** at any time to get out of Edit mode without saving your changes.*

4 To add a custom channel policy to the database, click **Add** (Add is disabled while in Edit mode).

*You can click **Reset** at any time to get out of Add mode without saving your changes.*

5 Enter the policy name.

6 Enter the policy description.

7 Configure channels 1-14 with Allow Ad Hoc (yes/no) and valid activity hours (Start Time/End Time).

8 Click **Commit** to save your input.

The table below lists the top fields in the in the **Create Policy: Channel** screen.

Field	Purpose
Select Channel Policy	This pick list displays all saved channel policies. Select a policy from this list, or you can click Add to edit your existing custom policy, or design a new policy. You can click **Delete** to remove channel policies. Included in the pick list is a Default policy (cannot be edited).
Policy Name	This displays the name of the policy.
Description	This displays a description of the policy.
Applied to Access Points	This memo field displays all Access Points currently configured to use the currently selected policy.
Channel Configurations	**Channel Number:** You must make configurations for each of the 14 channels. **Allow Ad Hoc:** Choose **Yes** to allow Ad Hoc; **No** to disallow Ad Hoc. Ad Hoc is independent of activity hours. *Note:* An ad hoc station is a User Station that is connected to one or more other User Stations without using an Access Point. Although ad hoc networking is a function of most standard 802.11 network client cards, User Stations that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network. **Valid Activity Hours:** For each channel, enter a **Start Time** and **End Time** in the input fields. *Note:* Enter times in a 24-hour format, using the format HH:MM. Traffic is *only* allowed between the start and end hours. Traffic detected on the channel outside this window generates an alarm.

Creating a No-Use Time-of-Day Channel Policy

To create an effective "no-use" time-of-day policy for a channel, enter a Start Time and End Time that are only one minute apart, e.g., 01:00 and 01:01. Entering 00:00 in *both* the Start Time and End Time *disables* alarm-generation for that channel.

Also, you may wish to explicitly set time-of-day and ad hoc policies for channels you know are not supposed to be in use. Even if you don't have a Sensor dedicated to scanning *all* channels, your deployed Sensors—even if locked onto just one channel—will hear network traffic bleeding over from adjacent channels, and will generate alarms based on them. This may assist you in tracking down unauthorized wireless users.

To apply the policies you created in Create Policies, you must access four program areas. These are:

- Global
- Sensor
- Access Point
- Station

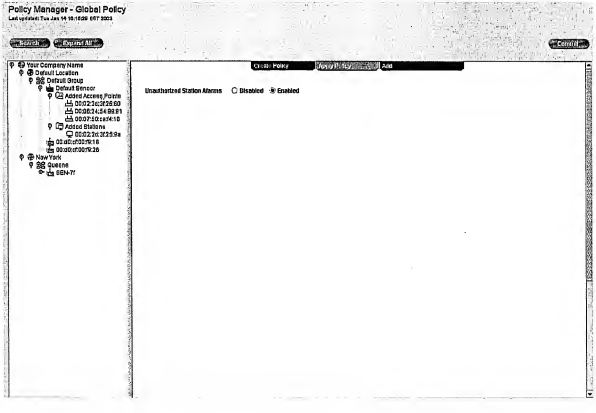
5.6.1 Apply Policy: Global

Use the **Apply Policy: Global** screen to disable or enable unauthorized Station alarms your WLAN.

> ***Note:*** Unauthorized Station alarms are generated for Stations that are associated with an authorized Access Point, but are not on that Access Point's list of valid Stations.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Global**



Steps to Use Apply Policy: Global

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Apply Policy: Global** *The Global Policy fields appears. The field has two selections: Enabled or Disabled.*
3	Click **Enable** to enable all unauthorized station alarms, or **Disable** to disable all unauthorized Station alarms in your WLAN.
4	Click **Commit.**

The table below lists the fields in the **Apply Policy: Global** screen.

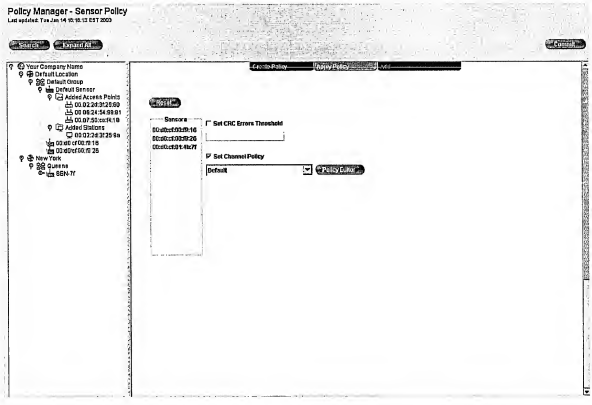
Field	Purpose
Unauthorized Station Alarms	• **Disabled:** Click **disable** and the AirDefense Server will **not** generate an alarm if it detects an unauthorized Station. • **Enabled:** Click **Enable** and the AirDefense Server will generate an alarm whenever it detects an unauthorized Stations in the portion of the WLAN the Sensor is monitoring.

5.6.2 Apply Policy: Sensor

Use **Apply Policy: Sensor** to apply your policies to the Sensors in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Sensor**



Steps to Use Apply Policy: Sensor

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Apply Policy: Sensor** *The Sensor Policy screen appears. This screen has three subscreens: A color-coded list of Sensors in your WLAN; Set CRC Errors Threshold; and Set Channel Policy.* ***Note:*** Clicking on the Policy Editor button takes you to the Channel Policy Editor (**Create Policy: Channel** screen). *You can click **Reset** at any time to get out of Edit mode without saving your changes.*
3	Click on the CRC Errors Threshold checkbox to enable the field, and enter the required information.
4	Click on the Set Channel Policy checkbox to enable the field, and enter the required information.
5	Click **Commit.**

The table below lists the fields in the Apply Policy: Sensor screen.

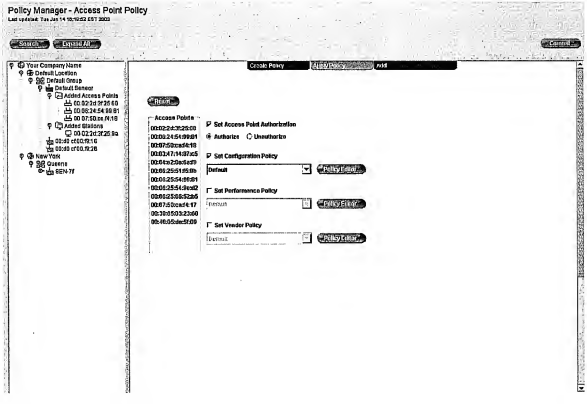
Field	Purpose
Sensors	This is a list of observed Sensors in your WLAN. The Sensor is color coded (see "Color Codes" on page 83).
Set CRC Errors Threshold	This is the threshold for the number of CRC errors allowed in WLAN the Sensor is monitoring. Enter a number of CRC errors per minute each Sensor may detect as it listens to the traffic in its reception area. High numbers of CRC errors may indicate that two or more Access Points are sharing the same channel; colliding with each other; that an object is interfering with the signal; or that a hacker may be flooding your air space with bad data in a Denial of Service attempt. *Note:* Unusually high numbers of CRC errors indicate network performance problems or the activity of a hacker.
Set Channel Policy	This pick list displays all saved channel policies. Select a policy from this list to apply to each Sensor in the Sensors list. Alternately, you can click Policy Editor to go to the Channel Policy Editor screen and edit, add, or delete channel policies. *Note:* Default policies cannot be edited.

5.6.3 Apply Policy: Access Point

Use **Apply Policy: Access Point** to apply your policies to one or more Access Points in your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Access Point**



Steps to Use Apply Policy: Access Point

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Apply Policy: Access Point** *The Access Point Policy fields appear. The main screen shows all Access Points in your WLAN.*
3	Select an Access Point to apply your policies to. *You can select configuration, performance, and vendor policies by clicking on the associated checkbox. Clicking Policy Editor takes you to the Configuration, Performance, and Vendor Policy Editing screens, where you can edit, add, and delete policies.* Policy Editor... *You can click **Reset** at any time to get out of Edit mode without saving your changes.*
4	Click **Commit.**

The table below lists the fields in the **Apply Policy: Access Point** screen.

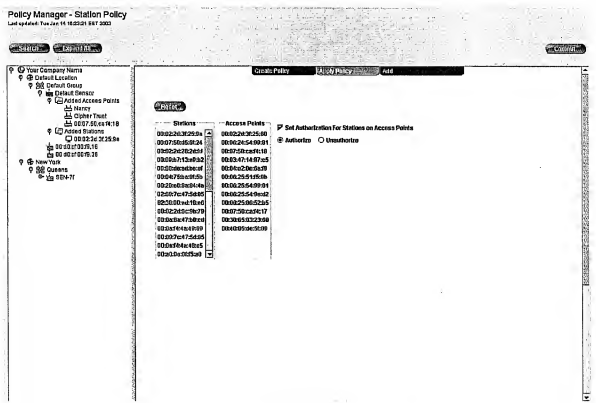
Field	Purpose
Access Points	This is a list of observed Access Points in your WLAN. *Note:* Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier.
Set Access Point Authorization	• **Authorize:** Select **Authorize** if this Access Point is a legitimate Access Point in your WLAN. • **Unauthorize**: Select **Unauthorize** if this Access Point is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever that Access Point is detected by a Sensor. (All detected Access Points *not authorized* are assumed to belong to hackers or violators of your wireless network policy.)
Set Configuration Policy	Clicking the checkbox allows you to select a default or custom configuration policy to apply to an Access Point. You can also click Policy Editor to go to the Configuration Policy Editor screen, where you can edit, add, or delete configuration policies.
Set Performance Policy	Clicking the checkbox allows you to select a default or custom performance policy for an Access Point. You can also click Policy Editor to go to the Performance Policy Editor screen, where you can edit, add, or delete performance policies.
Set Vendor Policy	Clicking the checkbox allows you to select a default or custom vendor policy for an Access Point. You can also click Policy Editor to go to the Vendor Policy Editor screen, where you can edit, add, or delete performance policies.

5.6.4 Apply Policy: Station

Use **Apply Policy: Station** to authorize or unauthorize Stations on Access Points in your WLAN. This feature allows you to authorize one Station on multiple Access Points. This useful feature allows you to authorize one user in the WLAN to use the network from multiple physical locations.

You can navigate to this screen by:

- Using the screen pull-down **Apply Policy: Station**



Steps to Use Apply Policy: Station

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Apply Policy: Station** *The Station Policy fields appear. The screen has three subscreens: An icon and color-coded list of Stations in your WLAN; an icon and color-coded list of Access Points your WLAN; and a field to authorize or de-authorize Stations on Access Points.*
3	Select a Station and the Access Point you wish to authorize or unauthorize.
4	Click the checkbox to open the field. • Select **Authorize** to authorize a Station on an Access Point. • Select **Unauthorize** to unauthorize a Station on an Access Point. *You can click **Reset** at any time to get out of Edit mode without saving your changes.*
5	Click **Commit.**

The table below lists the fields on the **Apply Policy: Station** screen.

Field	Purpose
Stations	This is a list of observed Stations in your WLAN. The Stations are icon and color coded (see "Color Codes" on page 83). ***Note:*** Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier.
Access Points	This is a list of observed Access Points in your WLAN. The Access Points are icon and color coded (see "Color Codes" on page 83). ***Note:*** Holding the mouse over an Access Point icon brings up a rollover screen that shows its Device Identifier.
Set Authorization for Stations on Access Points	• You must click on the checkbox before selecting authorize/unauthorize. • **Authorize:** Select **Authorize** if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. • **Unauthorize:** Select **Unauthorize** if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations *not authorized* are assumed to belong to hackers or violators of your wireless network policy.)

The Add/Import function of Policy Manager enables you to pre-configure and add Access Points and Stations to your WLAN manually, or by importing from a list of Access Points or Stations contained on a flat file. You can also use the Add/Import function to import user information.

Using **Policy Manager: Add/Import** will enable you to add Access Points and Stations to your WLAN that are already configured for authorization; configuration, performance, and vendor policies; and other operational behaviors.

You can use **Policy Manager: Add/Import** to:

- Pre-configure Access Points before adding them to your WLAN. This includes configuring the Access Point for authorized, unauthorize, or ignore; determining whether or not the Access Point is a bridge; and assigning or editing policies for the Access Point.
- Pre-configure Stations before adding them to your WLAN. This includes configuring the Station for a LEAP Username assignment (if applicable); placing the Station on a Watch or Ignore List; and authorizing or unauthorizing the Station for an Access Point.
- Import Access Points and Station MAC addresses from an ASCII comma-delimited flat file, and configure all of them prior to adding them to your WLAN.

Add has five screens. These are:

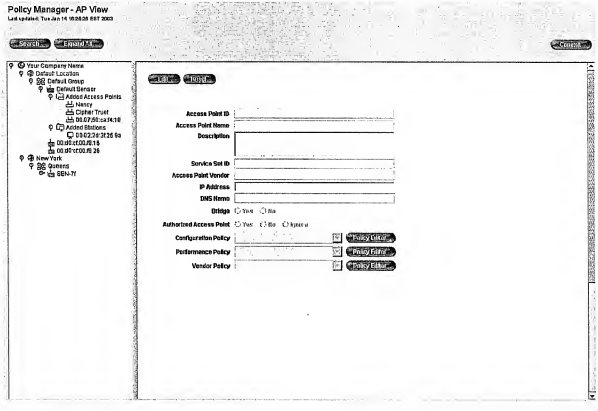
- Access Point
- Station
- Import Access Points
- Import Stations
- Import ACS Config

5.7.1 Add: Access Point

Use the **Add: Access Point** screen to manually pre-configure and add an Access Point to your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Add: Access Point**



Steps to Use Add: Access Point

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Add: Access Point** *The Add Access Point screen appears.*
3	Enter information into the open fields (see the table that follows for an explanation of each field). *You can select configuration, performance, and vendor policies by clicking on the associated checkbox. Clicking Policy Editor takes you to the Configuration, Performance, and Vendor Policy Editing screens, where you can edit, add, and delete policies.*
4	Click **Commit**.

The table below lists the fields in the Add: Access Point screen.

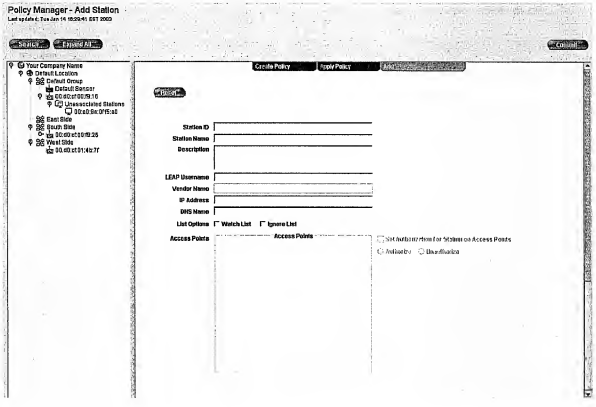
Field	Purpose
Access Point ID	MAC address of the Access Point. This is a required field.
Name	Name of the Access Point (optional)
Description	A description of the Access Point (optional)
Service Set ID	SSID number (this is not the same as the Access Point ID).
Access Point Vendor	Equipment manufacturer of the Access Point.
IP Address	The IP address of the Access Point.
DNS Name	The Access Point's DNS Name assignment (if applicable).
Bridge	• **Yes:** Click Yes if you are using this Access Point as a Bridge • **No:** Click No if you are not using this Access Point as a Bridge
Authorized Access Point	• **Yes:** Click **Yes** to authorize this Access Point for use in your WLAN • **No:** Click **No** to unauthorize this Access Point for use in your WLAN • **Ignore: Click** Ignore to place this Access Point in an Ignored state. *Note:* This feature is useful if you want to keep certain unauthorized Access Points or Stations your AirDefense Server sees from alarming, and thus preventing continuous false alarms. Sensors can detect Access Points in neighboring WLAN systems. When this happens, AirDefense generates an alarm. Designating an Access Point as Ignored prevents the Access Point and all Stations associated with the Access Point from alarming. If an attack occurs, an alarm generates regardless.
Configuration Policy	Leaving the default configuration policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Configuration Policy Editor screen if you wish to edit, add, or delete configuration policies.
Performance Policy	Leaving the default performance policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Performance Policy Editor screen if you wish to edit, add, or delete performance policies. 
Vendor Policy	Leaving the default vendor policy for the Access Point in place, or specify a custom policy. Click **Policy Editor** to go to the Vendor Policy Editor screen if you wish to edit, add, or delete vendor policies. 

5.7.2 Add: Station

Use the **Add: Station** screen to manually pre-configure and add a Station to your WLAN.

You can navigate to this screen by:

- Using the screen pull-down **Add: Station**



Steps to Use Add: **Station**

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Add: Station** *The Add Station screen appears.*
3	Enter information into the open fields (see the table that follows for an explanation of each field).
4	Click **Commit**.

Add Station displays the following.

Field	Displays...
Station ID	The MAC address of the Station. AirDefense automatically generates this field.
Name	The Name of the Station (optional)
Description	A description of the Station (optional)
LEAP Username	The LEAP Username. This field applies if you are using EAP Configuration Mode in your configuration policy definition. (See "Create Policy: Configuration" on page 99.)
Vendor Name	The equipment manufacturer of the Station. AirDefense automatically generates this field.
IP Address	The IP address of the Station.
DNS Name	The Station's DNS Name assignment (if applicable).
List Options	If you are going to use a List Option, the option must be either Watch List, or Ignore. • **Watch List:** Click on this checkbox if you wish to know if this Station's MAC address will occur in your network again. The next time the AirDefense Server sees this Station, it will generate an alarm for every minute the it sees this Station's in the network. The Watch list is unrelated to authorized/unauthorized states. • **Ignore List:** Click on this checkbox if you wish the AirDefense Server to ignore the presence of a Station on the network. AirDefense does not generate an alarm for any devices on the Ignore list. ***Note:*** This feature is useful if you want to keep certain unauthorized Stations that your AirDefense Server sees from alarming, as in the case of Stations in an adjacent office that belong to another Company. Placing these known "friendly" Stations on the Ignore list prevents continuous false alarms.
Access Points	List of Access Points that the Station is associated with.
Set Authorization For Station on Access Points	• You must click on the checkbox before selecting authorize/unauthorize. • **Authorize:** Select **Authorize** if this Station is a legitimate Station assigned to an legitimate Access Point in your WLAN. • **Unauthorize:** Select **Unauthorize** if this Station is not legitimate. If it is not authorized here, the AirDefense Server will generate an alarm once a minute whenever a Sensor detects the Station. (All detected Stations *not authorized* are assumed to belong to hackers or violators of your wireless network policy.)

5.7.3 Add: Import Access Points

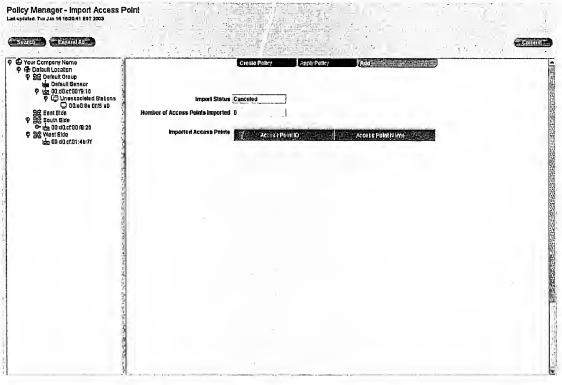
Use the **Add: Import Access Points** screen to import an Access Points into your WLAN.

Note: When you import an Access Point that has never been seen by AirDefense, it will appear as Blue (unassociated) in Tree View. Once AirDefense sees the Access Point, the Access Point will become Green (if you authorized it prior to import), or Red (if you did not authorize it prior to import). The Access Point will move to an associated location in the tree.

Important: AirDefense rejects any file that is not in the correct format or if you have exceeded your license agreement count. See Appendix B: File Import Formats for the correct file format. See Chapter 8, Administration, on page 217 for information regarding license agreements.

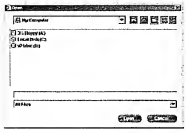
You can navigate to this screen by:

- Using the screen pull-down **Add: Import Access Points**



Steps to Use Add: Import Access Points

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Add: Import Access Points**
	A browser window appear



3 Navigate to the desired file, and select the file.

4 Click **Commit**.

Import Access Points displays the following:

Field	Displays...
Import Status	The status of the current import.
Number of Access Points Imported	The number of Access Points being imported into AirDefense.
Imported Access Points	**Access Point ID:** The Device Identifier of the Access Point. **Access Point Name:** The user-configured name of the Access Point.

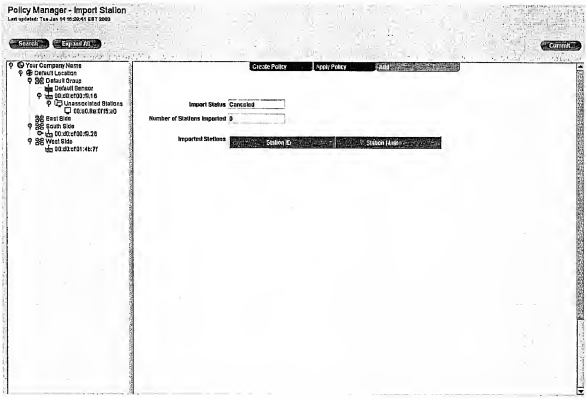
5.7.4 Add: Import Stations

Use the **Add: Import Stations** screen to import a list of Stations into your WLAN.

> ***Important:*** When you import a station, it overwrites all information that is already in AirDefense. AirDefense rejects any file that is not in the correct format. See Appendix B: File Import Formats for the correct file format.

You can navigate to this screen by:

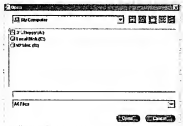
- Using the screen pull-down **Add: Import Stations**



***Steps to Use Add: Import* Stations**

To use the **Add: Import Stations** screen, do the following:

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Add: Import Stations** *A browser window appears.*



3 Navigate to the desired file, and select the file.

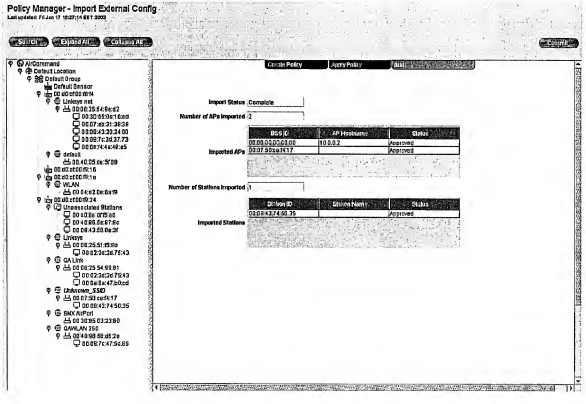
4 Click **Commit**.

Import Stations displays the following:

Field	Displays...
Import Status	The status of the current import.
Number of Stations Imported	The number of Stations being imported into AirDefense.
Imported Stations	**Access Point ID:** The Device Identifier of the Station. **Access Point Name:** The user-configured name of the Station.

5.7.5 Import ACS Config

Use **Add: Import ACS Config** to import Access Points and Stations into AirDefense from a Cisco Access Control Server.



Prerequisites to Use Add: Import ACS Config

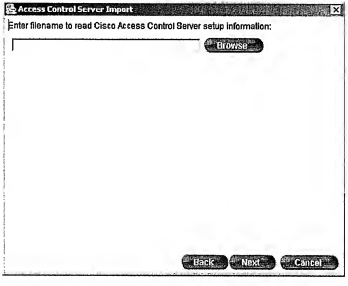
To use Add: Import ACS Config, you must have downloaded two.txt files into your workstation. These files are:

- Import Access Control Server **Setup** File
- Access Control Server **Dump** File

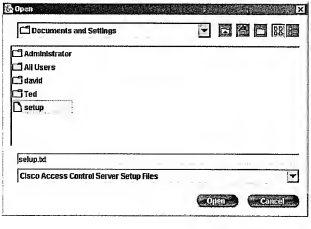
You can get these files from Cisco, form the server that is running ACS, using their command line tool.

Steps to Use Add: Import ACS Config

Step	Action
1	Select the AirDefense (top) level of Tree View.
2	Click and pull down **Add: import ACS Config.** *The following window appears.*

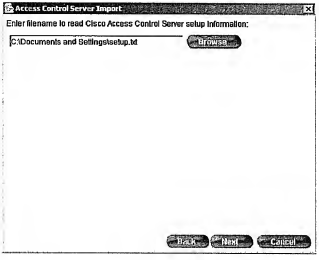


3 Find the data.txt file. Click Browse to find the file in your database directory.
A Browser window appears.



4 Select the **Setup.txt** file and click **Open**.

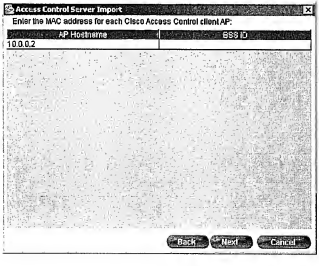
The following window appears, showing the path with Setup.txt file.



5 Click **Next**.

This reads the setup file, which contains the Hostname and other information about the Cisco Access Control Access Point--the Access Point that directly connects to the Cisco Control Server. This is an authentication step.

The following window appears.



6 Double-click in BSS ID column. In this column, enter the MAC address of each Access Point Hostname that appears.

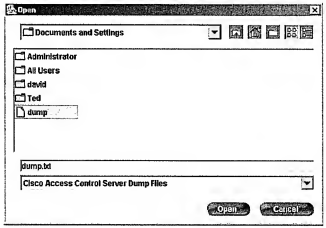
Note: If you do not enter a valid MAC address for each Access Point, you cannot proceed.

7 Click **Next**.

The following window appears

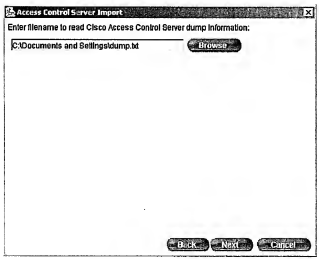
8 Find the dump.txt file. Click Browse to find the file in your database directory.

A Browser window appears.



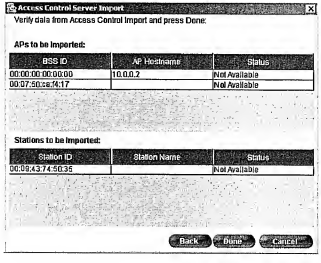
9 Select the **Dump.txt** file and click **Open.**

The path with Dump.txt file appears in the Access Control Server Import window.



10 Click **Next.**

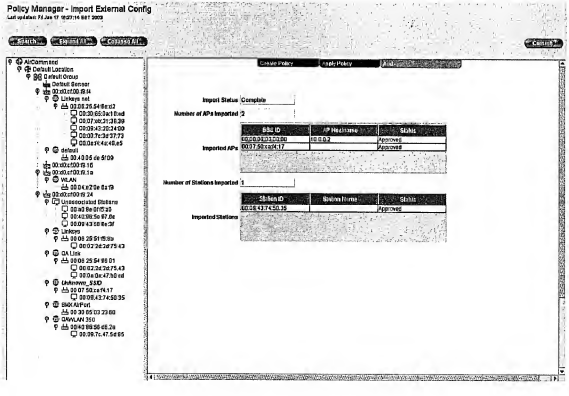
The following window appears, which lists Access Points and Stations to be imported.



11 Click **Done.**

Alternately, you can click ***Cancel*** *to leave the window with no changes.*

The Import External Config screen appears, with fields populated.



12 Click **Commit** to save all changes.

Import ACS Config. displays the following:

Field	Displays...
Import Status	The status of the current import. • **Pending:** Import is in process • **Cancelled:** Import was cancelled • **Complete:** Import is complete
Number of APs Imported	The number of Access Points being imported into AirDefense.
Imported APs	Information on the imported Access Points. • **BSS ID:** The MAC address of the Access Point. • **AP Host Name:** The user-configured name of the Access Point. This depends on what is entered into the Cisco server. For Access Points, this is usually the IP address. • **Status:** Information on licensing. — **Not available:** Licensing not available for Access Points being imported — **Approved:** Licensing approved for Access Points being imported — **Denied:** License exceeded
Number of Stations Imported	The number of Stations being imported into AirDefense.
Imported Stations	Information on the imported Stations. • **Station ID:** The Device Identifier of the Station. • **Station Name:** The user-configured name of the Station • **Status:** Information on licensing. — **Not available:** Licensing not available for Stations being imported — **Approved:** Licensing approved for Stations being imported — **Denied:** License exceeded

6 Notification Manager

Use Notification Manager to specify how AirDefense should deliver its alarms and reports to a designated administrator.

AirDefense generates a variety of alarms that immediately let the administrator know when irregular or unauthorized wireless network activity occurs. In addition, AirDefense generates daily reports of network traffic and security concerns.

Note: All reports are in html format.

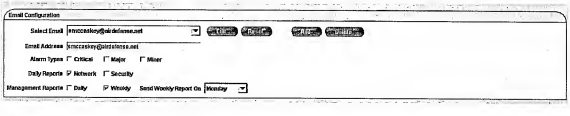
6.0.1 In This Chapter

This chapter contains the following topics.

6.1 Email Configuration

Use the Email Configuration table to configure options for the individuals you want to receive of alarm and report notifications by email.

- Alarm Notifications are specific alarms generated by policy violations and other irregularities that AirDefense detects.
- Reports summarize network activity and network security violations. There are two types of reports:
  - — Daily Reports on Network and Security Violations
  - — Management Reports



The table below describes the fields in the Email Configuration table.

Field	Description
Select Email	Select the IP address of the person (or persons) you want to receive alarm and report notifications. *Note:* You may send both alarms and reports by email to an unlimited number of users For each selected user, you can choose the alarms or reports you want to receive from the Alarm and Report Types check boxes. AirDefense emails notifications to the IP address provided.
Email Address	Once you Select Email, the IP address of the recipient should appear in this field.
Alarm Types	Click one, two, or all three checkboxes to filter the type of reports that will appear in the email notifications. AirDefense detects a range of wireless network attacks and policy violations and prioritizes all alarms into three types: • **Critical**—Alarms that should receive immediate attention • **Major**—Alarms that suggest potentially serious problems • **Minor**—Alarms that simply inform, or suggest potential problems
Daily Reports	Click one or both checkboxs. • **Network:** Choose Network to receive reports on network activity. • **Security:** Choose Security to receive security reports.
Management Reports	Click one or both checkboxs. • **Daily:** Click Daily to receive Management Reports every day. • **Weekly:** Click Weekly to receive Management Reports every week.If you select this option, you must then select the day you want to receive the report. Send Weekly Report On Monday

Management Reports

Management email reports give trend analysis information on general security vulnerabilities, network health, and performance, and security policy management. The reports you receive apply to AirDefense trends for current week, and can extend back to up to four weeks. Management reports contain information from the following reports: Device List, Threat Summary, Policy Summary, and Health Summary.

6.1.1 Editing Email Options

Steps to Edit an Existing Recipient's Email Options

Step	Action
1	Select the recipient's address from the Select Email pick list and click **Edit**. *This enables the input fields. To cancel any changes and return to non-edit mode, click* ***Reset.***
2	Make any changes, as needed, to the fields: • Alarm Type • Daily Report • Management Report (if you select this option, you must also select a day to receive the reports. *Alternately, click* ***Delete*** *to permanently remove the selected email address and associated options.*
3	Click **Commit** to save the changes.

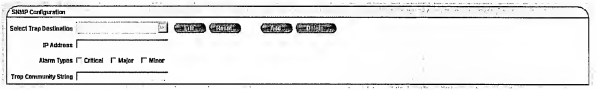
Steps to Create a New Email Recipient

Step	Action
1	Click **Add** and enter an email address in the Email Address input field. ***Note:*** The input field only accepts one address at a time.
2	Configure the following fields: • Alarm Types • Daily Report • Management Report (if you select this option, you must also select a day to receive the reports.
3	Click **Commit**
4	Click **Add** to create a new email recipient.

AirDefense can send traps to your SNMP AirDefense Server. Use the SNMP Configuration table to configure SNMP notifications.

Note: Before your SNMP AirDefense Server can process its traps completely, however, you must build AirDefense's MIB (message information block) file in your SNMP software. Unless you build the MIB file, only a portion of the AirDefense alarm information will display in your SNMP utility.

Note: AirDefense provides a MIB for your convenience. The MIB file can be found at:**/usr/smx/local/mib**



The table below describes the fields in the SNMP Configuration table.

Field	Description
Select Trap Destination	Select the destination.
IP Address	Enter the IP address of your SNMP AirDefense Server. The input field only accepts one address at a time.
Alarm Types	Click one, two, or all three checkboxes to filter the type of reports that will appear in the SNMP notifications. AirDefense detects a range of wireless network attacks and policy violations and prioritizes all alarms into three types: • **Critical**—Alarms that should receive immediate attention • **Major**—Alarms that suggest potentially serious problems • **Minor**—Alarms that simply inform, or suggest potential problems
Trap Community String	Enter your trap community string.

6.2.1 Copying the AirDefense MIB File

Steps to Copy the AirDefense MIB File

Step	Action
1	Log onto the AirDefense Server via an SSH client (see "Installing the AirDefense Server" on page 1).
2	Copy the following file to a location where your SNMP (V2) software can import it for compilation: **usr/smx/local/mib.**

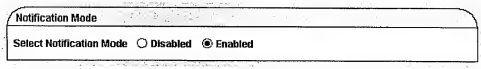
6.2.2 Configuring AirDefense for SNMP

Steps to Configure AirDefense for SNMP

Step	Action
1	Click **Add** to edit the IP address input field. ***Note:*** The input field only accepts one address at a time.
2	Configure the following fields: • Alarm Types • Trap Community String
3	Click **Commit**
4	Click **Add** to add additional SNMP AirDefense Server IP addresses.

6.3 Notification Mode

Use the Notification Mode table to toggle alarm notifications on or off.



The table below describes the fields in the Notification Mode table.

Field	Description
Disabled	Click **Disable** to turn alarm notifications off. This effects both email and SNMP alarms.
Enabled	Click **Enabled** to turn alarm notifications on. This effects both email and SNMP alarms.

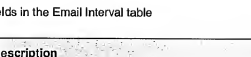
6.4 Email Interval

Email intervals are the minutes that separate email notifications, ***not*** notifications per hour.

Note: Email rate control does not apply to daily reports.They are generated and emailed once a day.

Use the pull down to enter the email interval.

Example: *If you select ten minutes, AirDefense will send an email every ten minutes—the email will contain all alarms generated during the past ten minutes.*



The table below describes the fields in the Email Interval table

Field	Description
Minutes between Msgs	Choose the email interval in minutes from the pull down. There are seven choices in the pull-down: 1, 5, 10, 15, 20, 30, and 60.

SNMP intervals are the minutes that separate SNMP notification, ***not*** notifications per hour.

Use the pull down to enter the number of minutes between SNMP traps.

The table below describes the fields in the Email Interval table

Field	Description
Minutes between Msgs	Choose the SNMP interval in minutes from the pull down. There are seven choices in the pull-down: 1, 5, 10, 15, 20, 30, and 60.

6.6 Content of Email Notifications

There are four types of email notifications:

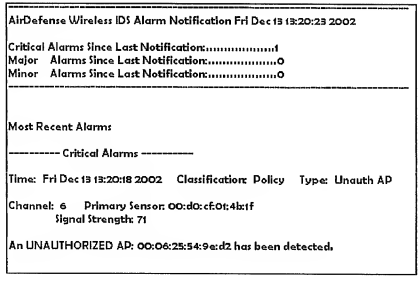
- Alarm Notification
- Daily Security Report
- Daily Network Report
- Management Report

Alarm Notification

The Alarm Notification contains the following information:

- Critical, Major, and Minor alarms since the last notification
- Information about the most recent alarms per channel, including:
  - — Time and data stamp
  - — Alarm classification
  - — Alarm type
  - — Channel number
  - — Primary Sensor MAC address
  - — Signal Strength
  - — Unauthorized AP identification

The illustration on the next page shows a typical Alarm Notification.



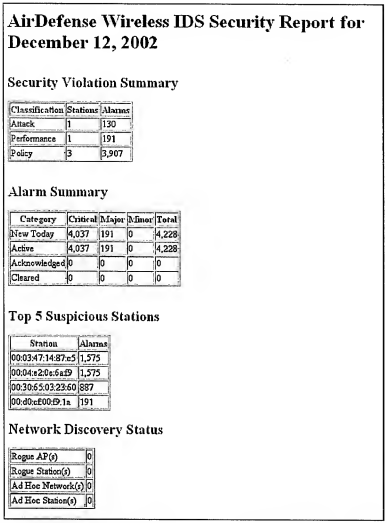
Daily Security Report

The Daily Security Report contains the following information:

Security Violation Summary

- Alarm Summary
- Top 5 Suspicious Stations
- Network Discovery Status

The illustration on the next page shows a typical Daily Security Report.



AirDefense Wireless IDS Security Report for December 12, 2002

Security Violation Summary

Classification	Stations	Alarms
Attack	1	130
Performance	1	191
Policy	3	3,907

Alarm Summary

Category	Critical	Major	Minor	Total
New Today	4,037	191	0	4,228
Active	4,037	191	0	4,228
Acknowledged	0	0	0	0
Cleared	0	0	0	0

Top 5 Suspicious Stations

Station	Alarms
00:03:47:14:87:e5	1,575
00:04:e2:0e:6a:f9	1,575
00:30:65:03:22:60	887
00:d0:cf:00:f9:1a	191

Network Discovery Status

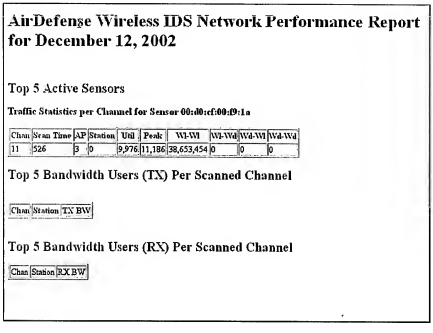
Rogue AP(s)	0
Rogue Station(s)	0
Ad Hoc Network(s)	0
Ad Hoc Station(s)	0

Daily Network Report

The Daily Network Report contains the following information:

- Top 5 active Sensors
- Traffic Statistics per Channel for Sensor
- Top 5 Bandwidth Users Transmitted Per Scanned Channel
- Top 5 Bandwidth Users Received Per Scanned Channel

The illustration below shows a typical Daily Network Report.



AirDefense Wireless IDS Network Performance Report for December 12, 2002

Top 5 Active Sensors

Traffic Statistics per Channel for Sensor 00:d0:cf:00:f9:1a

Chan	Scan Time	AP	Station	Util	Peak	Wi-Wi	Wi-Wd	Wd-Wi	Wd-Wd
11	526	3	0	9,976	11,186	38,653,454	0	0	0

Top 5 Bandwidth Users (TX) Per Scanned Channel

Chan	Station	TX BW

Top 5 Bandwidth Users (RX) Per Scanned Channel

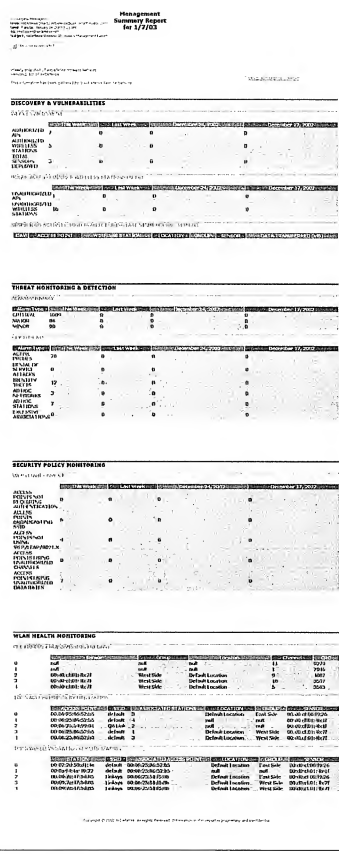
Chan	Station	RX BW

Management Report

The Management Report contains the following information:

- Discovery & Vulnerabilities
  - — WLAN Environment
  - — Rogue Access Points and Wireless Stations Found
  - — Suspicious Activity: High Traffic During Late Night Hours - Top Five
- Threat Monitoring & Detection
  - — Alarm Summary
  - — Key Threats
- Security Policy Monitoring
  - — WLAN Environment
- WLAN Health Monitoring
  - — CRC Errors (Transmission Errors)
  - — Top 5 Access Points by Utilization
  - — Top 5 Wireless Stations by Utilization

The illustration on the next page shows a typical Management Report.


Management
Summary Report
for 1/2/03
DISCOVERY & VULNERABILITIES
THREAT MONITORING & DETECTION
SECURITY POLICY MONITORING
WLAN HEALTH MONITORING

SNMP Notifications contain the following information.

Information about the most recent alarms per channel, including:

- Time and data stamp
- Alarm classification
- Alarm type
- Channel number
- Primary Sensor MAC address
- Signal Strength
- Unauthorized AP identification

Note: The format that SNMP Notification data is output by an SNMP AirDefense Server is dependent on the AirDefense Server configuration, i.e., how the AirDefense Server generates text files.

7 Reports

AirDefense provides detailed reports that contain information about your WLAN. There are four major report categories:

- Summary
- Sensor
- Access Point
- Station

7.0.1 In This Chapter

This chapter contains the following topics.

The table below summarizes the reports.

Report	Description
Summary	• **Device Summary:** Summarizes all authorized and unauthorized devices on your WLAN • **Device List:** Displays all devices that are currently active in your WLAN on any given date, by device and type • **Missing Devices:** Displays ID information about Access Points and Stations that the Sensor can no longer see. • **Threat Summary:** Summarizes activities that are threatening the network: alarm summaries, network probes, and after hour activities • **Policy Summary:** Summarizes policy monitoring for Access Nodes in your WLAN • **Health Summary:** Shows a comprehensive health report on device activities, such as downtime and use statistics, noisiest channels, and frequency of use statistics for Access Points and Stations • **Ad Hoc Networks:** Shows the Access Points and Stations currently engaged in Ad Hoc networking, by MAC address/Name, Group, Location, and Sensor • **Rogue Summary:** Shows details on the Access Points and Stations that are unauthorized for use in the WLAN.
Sensor	• **Sensor Current View:** Displays counts of alarms generated by Sensor, Group, and Location • **Sensor Channel View:** Displays network statistics for each channel, filtered by Sensors. The display includes which Access Points, Stations, or ad hoc networks were detected on specific channels, how many bytes of data were transmitted • **Sensor Performance View:** Displays a daily overview of your network statistics per channel based on selected Sensors
Access Point	• **AP Summary:** Display summaries of network traffic statistics for each Access Point • **AP Statistics:** Displays minute-by-minute network traffic statistics for each Access Point • **AP Policy Violations:** Displays information on APs that are in violation of policies • **Unauthorized APs:** Displays all Access Points and Stations are not authorized on the WLAN, by MAC address/Name, Group, Location, and Sensor
Station	• **Station Summary View:** Displays summaries of network traffic statistics for each Station • **Station Current View:** Displays network traffic statistics for each station for the most recent minute • **Single Station View:** Displays minute-by-minute network traffic statistics for a single Station • **Probing Stations:** Displays identification information on Stations in the WLAN being probed for weaknesses

Report Manager enables you to access reports easily from pull-down menus, filter reports using different criteria, and save and print reports using either comma-separated values or html.

7.2.1 Accessing Reports

Four tabs beneath the main navigation icons at the top of the page provide access to all report categories. Clicking each tab displays sub-menus to view the specific reports:

7.2.2 Viewing Reports

Steps to View Reports

Step	Action
1	On any page, view reports by selecting a date from the date pick list.
2	Click **Load.**
	The date filter you select will persist for all other Reports you view in the Reports program area, until you specifically select another date.

Note: AirDefense deletes data used to create these reports after thirty days

7.2.3 Filtering Reports

Steps to Filter Reports

Step	Action
1	Select **Custom...** from the **Date** pick list to specify a select range of hours whose data you want to view.
	A date window appears.
2	Select a date, a start hour, and an end hour, in the available pick lists.
3	On any page (except Sensor Current View and Single Station View), click **Filter** to select a Sensor.
	The data for whose monitored Access Points will be displayed.

Note: For the Sensor channel view report, you must select a Sensor before the date can be loaded, since the report is per Sensor. Other reports can be displayed for all Sensors, or filtered by location, by groups, or by individual Sensor.

Note: On any page containing a list of Access Points, resting your mouse over a particular Access Point causes the SSID to which it belongs to popup in a small window.

7.2.4 Printing Reports

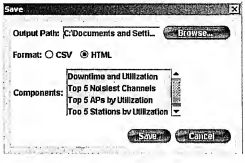
Reports gives you a print option that you can use to save the content of reports to your local system for printing. You can print the content in the following formats:

- Comma-separated value (CSV)
- html

Note: The printed report has the same look and feel as the notification reports you can elect to receive via email (see See "Notification Manager" on page 137.)

Steps to Print Reports

Step	Action
1	Click **Save** on the Reports screen 
	The Save screen appears.
2	Click **Browse** to choose the output path to your local system.
3	Click on the format you want to print in: • **CSV** (comma-separated value) • **HTML**
4	Select the report you want to print, from the Components list.
5	Click **Save**. *Alternately, you can click **Cancel** to cancel without changes.*



Click the Summary tab to reveal the Summary reports. There are seven possible Summary reports--see the table below.

Summary Report	Description
Device Summary	Summarizes of all authorized and unauthorized network elements on your WLAN. The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications).
Device List	Shows a list of devices (network elements) that are currently active in your WLAN. The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications)
Missing Devices	List s ID information about Access Points and Stations that the Sensor can no longer see.
Threat Summary	Summarizes activities that are threatening the network: alarm summaries, network probes, and after hour activities
Policy Summary	Summarizes policy monitoring for Access Nodes in your WLAN.The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications).
Health Summary	Shows a comprehensive health report on WLAN activities, such as downtime and use statistics, noisiest channels, and frequency of use statistics for Access Points and Stations.The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications).
Ad Hoc Networks	Shows the Access Points and Stations currently engaged in Ad Hoc networking, by MAC address/Name, Group, Location, and Sensor.
Rogue Summary	Shows details on the Access Points and Stations that are unauthorized for use in the WLAN.

7.3.1 Device Summary

Device Summary enables you to view the following for any date you choose.

- **WLAN Environment:** The number of authorized Access Points, Stations, and Sensors currently deployed in your WLAN.
- **Rogue APs and Stations Found:** The number of unauthorized (rogue) Access Points and Stations currently being detected in your WLAN.

  Note: The contents of this report is the same as contained in the daily and weekly management reports (see Chapter 6, Notification Manager for more information on email notifications).

Steps to Use Device Summary

To use Device Summary choose the desired date from the date pick list and click **Load.**

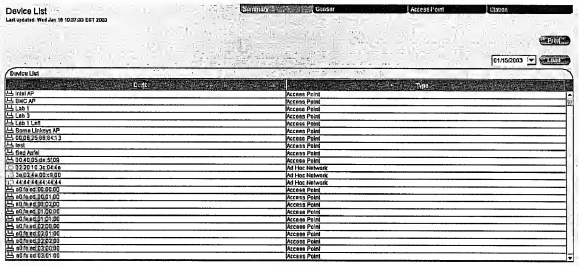
Device Summary displays the following information.

Field	Displays...
WLAN Environment	• **Authorized APs:** The number of Access Points that are authorized for use in your WLAN • **Authorized Stations:** The number of Stations that are authorized for use with Access Points in your WLAN • **Total Sensors Deployed:** The total number of Sensors currently deployed in your WLAN.
Rogue APs and Stations Found	• **Unauthorized APs:** The number of Access Points that the Sensor sees, but that are unauthorized for use in the WLAN. • **Unauthorized Stations:** The number of Stations that the Sensor sees, but that are unauthorized for use with Access Points in the WLAN.

7.3.2 Device List

Device List enables you to view all devices that are currently active in your WLAN on any given date, by Device Identifier and Type.

> ***Note:*** The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications).



Steps to Use Device List

To use Device List choose a date from the date pick list, and click **Load**

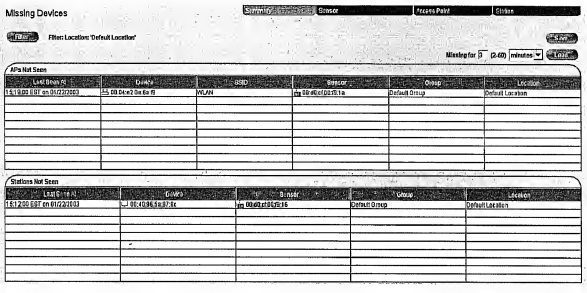
Device List displays the following information.

Column	Displays...
Device (Identifier)	The color-coded icon of the device, and its name if applicable. ***Note:*** Hover the mouse over the icon to reveal a rollover screen that displays the icon's Device Identifier.
(Device) Type	The type of device: Sensor, Access Point, Bridged Access Point, or Station.

7.3.3 Missing Devices

Missing Devices displays information about Access Points and Stations that the Sensor no longer sees.

- **APs Not Seen**
- **Stations Not Seen**

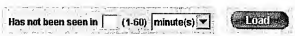


Steps to Use Missing Devices

To use Missing Devices, do the following:

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears.*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK**.

4	Select a date from the date pick list and click **Load**



APs Not Seen

APs Not Seen displays the following:

Column	Displays...
Last Seen At	The time and date the Access Point was seen by the Sensor.
Device	The color-coded icon and the Device Identifier of the Access Point.
SSID	The (Extended) Service Set ID (SSID) of the Access Point, if available.
Sensor	The color-coded icon and the Device Identifier of the Sensor.
Group	The Group the Sensor belongs to.
Location	The Location the Sensor belongs to.

Stations Not Seen

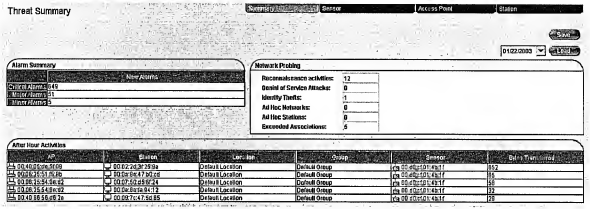
Stations Not Seen displays the following:

Column	Displays...
Last Seen At	The time and date the Access Point was seen by the Sensor.
Device	The color-coded icon and Device Identifier of the Station.
Sensor	The Sensor the Station is associated with.
Group	The Group the Sensor belongs to.
Location	The Location the Sensor belongs to.

7.3.4 Threat Summary

Threat Summary summarizes activities that are threatening the network. The screen shows three tables:

- Alarm Summary
- Network Probing
- After Hour Activities



Steps to Use Threat Summary

To use Threat Summary, select a date from the date pick list and click **Load**.

Alarm Summary

Alarm Summary shows the number of Critical, Major, and Minor priority alarms in AirDefense for the selected date. It displays the following:

Note: For more information on alarms, see Chapter 3, Alarm Manager.

Field	Displays...
Critical	The number of Critical alarms for the selected date. Critical alarms should receive immediate attention.
Major	The number of Major alarms for the selected date. Major alarms are potentially serious.
Minor	The number of Minor alarms for the selected date. Minor alarms suggest potential problems.

Network Probing

Network Probing displays the frequency of network probes directed against the WLAN for the specified data. It displays the following:

Field	Displays...
Reconnaissance Activities	The frequency of reconnaissance activities taking place on your WLAN
Denial of Service Attacks	The frequency of a Denial of Service attacks taking place on your WLAN. Denial of Service attacks take place when an attacker spoofs the MAC address of an Access Point and either tells a specific host or all hosts to disassociate.
Identity Thefts	The frequency of attempts of identity theft taking place on your WLAN.
Ad Hoc Networks	The number of Ad Hoc Networks currently engaged on your WLAN.
Ad Hoc Stations	The number of Ad Hoc Stations currently engaged on your WLAN.
Exceeded Associations	The number of exceeded associations taking place on your WLAN.

After Hour Activities

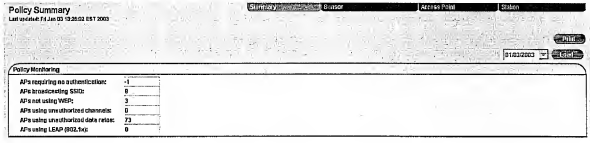
The After Hour Activities table displays the identity of those Access Points and Stations that are engaged in after hours activities. The After Hour Activities table displays the following:

Field	Displays...
AP	The Access Point used during the after hours session.
Station	The Station associated with the Access Point used in the after hours session.
Location	The Location of the Sensor that detected the after hours session.
Group	The Group designation for the Sensor that detected the after hours session.
Sensor	The Sensor ID of the Sensor that detected the after hours session.
BytesTransferred	The amount of data transferred, in Megabytes, during the after hours session.

7.3.5 Policy Summary

Policy Summary displays a summary of your policy selections for the Access Nodes in your WLAN. The policies in the table correspond to the policies you configured for each Access Point in Policy Manager. (For more information on configuring policies for Access Points, see "Create Policy: Configuration" on page 99.

Note: The contents of this report is the same as contained in the daily and weekly management reports (see Chapter 6, Notification Manager for more information on email notifications).



Steps to Use Policy Summary

To Use Policy Summary, select a date from the date pick list and click **Load**.

The Policy Summary screen displays the following:

Field	Displays...
APs requiring no authentication	The number of Access Points that do not require authentication. *Note:* This type of Access Point can accept non-authenticated network connections, allowing any Station to associate with it. This generates alarms. For more information, see "Create Policy: Configuration" on page 99.
APs broadcasting SSID	The number of Access Points that are broadcasting SSIDs in their beacon. *Note:* To configure the SSID beacon, see "Create Policy: Configuration" on page 99.
APs not using WEP	The number of Access Points that are not using Wired Equivalent Privacy (WEP). *Note:* As a minimal security measure, you should enable Wired Equivalent Privacy (WEP) on every Access Point. To do this, see "Create Policy: Configuration" on page 99.
APs using unauthorized channels	The number of Access Points that are using unauthorized channels. *Note:* For more information on channel configuration, see "Create Policy: Channel" on page 112.

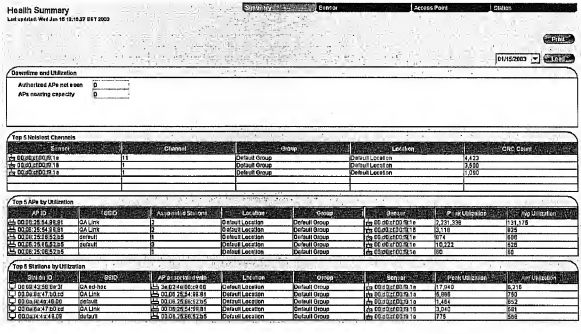
Field	Displays...
APs using unauthorized data rates	Displays the number of Access Points that are using unauthorized data rates. *Note:* Each Access Point is configured to transmit and receive data at specified rates. If AirDefense detects the Access Point transmitting or receiving data at a disallowed rate, it generates an alarm. For more information, see "Create Policy: Configuration" on page 99.
APs using LEAP (802.1x)	Displays the number of Access Points that are using LEAP (EAP authentication mode). *Note:* Using this in the policy definition ensures that LEAP is deployed and being used by both Access Points and Stations. If an Access Point or Station is not configured correctly and not running LEAP, AirDefense generates an alarm for either instance. For more information, see "Create Policy: Configuration" on page 99.

7.3.6 Health Summary

Health Summary displays a comprehensive health report on WLAN activities. It contains four tables:

- Downtime and Utilization
- Top 5 Noisiest Channels
- Top 5 APs by Utilization
- Top 5 Stations by Utilization

Note: The contents of this report is the same as contained in the daily and weekly management reports (see Notification Manager for more information on email notifications).



Steps to Use Health Summary

To use Health Summary, select a date from the date pick list and click **Load.**

Downtime and Utilization

Downtime and Utilization displays the following:

Field	Displays...
Authorized APs not seen	The number of Access Points that are authorized on the WLAN, but are not being detected by a Sensor.
APs nearing capacity	The number of Access Points on the WLAN that are nearing their capacity to receive and transmit data.

Top 5 Noisiest Channels

Top 5 Noisiest Channels displays the following:

Column	Displays
Sensor	The Sensor that has one or more noisy channels.
Channel	The Channel number on the Sensor that is the nosiest channel.
Group	The Sensor's Group association.
Location	The Sensor's Location association.
CRC Count	The total number of CRC errors detected, since midnight.

Top 5 APs by Utilization

Top 4 APs by Utilization displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point.
Associated Stations	The Stations that are associated with each Access Point.
Location	The Access Point's Location association.
Group	The Access Point's Group association.
Sensor	The Access Points Sensor association.
Peak Utilization	The Access Point's highest usage in bytes.
Avg Utilization	The Access Point's average usage in bytes.

Top 5 Stations by Utilization

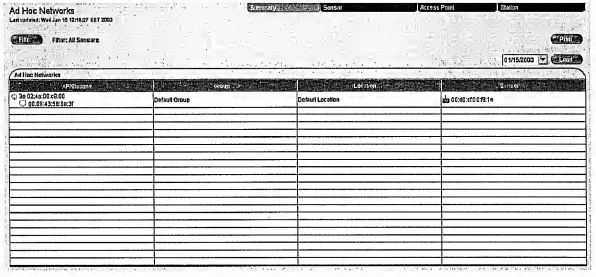
The Top 5 Stations by Utilization table displays the following:

Column	Displays...
Station ID	The Device Identifier of the Station.
SSID	The Access Point SSID of the Access Point associated with the Station.
AP associated with	The Access Point associations that exist in the network.
Location	The Station's Location association.

Column	Displays...
Group	The Station's Group association.
Sensor	The Sensor the Station is associated with.
Peak Utilization	The highest level of usage in bytes.
Avg Utilization	The average level of usage in bytes.

7.3.7 Ad Hoc Networks

Ad Hoc Networks display information on the Access Points and Stations currently engaged in Ad Hoc networking, by MAC address/Name, Group, Location, and Sensor.



Steps to Use Ad Hoc Networks

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK.**

Step	Action
4	Select a date from the date pick list and click **Load**

The Ad Hoc Networks screen displays the following:

Column	Displays...
AP/Stations	The color-coded icon and Device Identifier of the Access Point or Station that is engaged in Ad Hoc networking.
Location	The Location of the Sensor that detects the Access Points and Stations engaged in Ad Hoc networking.
Group	The associated Group.
Sensor	The color-coded icon and Device Identifier of the associated Sensor.

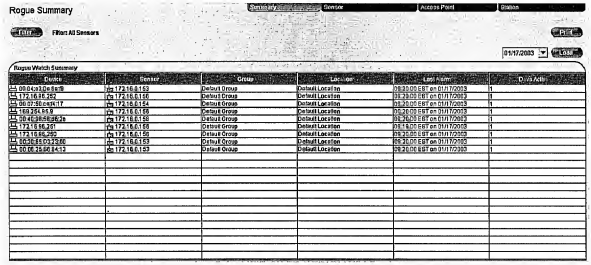
7.3.8 Rogue Summary

Rogue Summary displays information on the Access Points and Stations that are currently unauthorized for use on the WLAN. Rogue devices can be illegally installed devices.

Note: The number of rogue Access Points and Stations is reported in the Device Summary.

- Unauthorized Access Points are Access Points that the Sensor sees, but that are unauthorized for use in the WLAN.
- Unauthorized Stations are Stations that are unauthorized for use with Access Points in the WLAN.

Example: *A rogue Access Point generates an Unauthorized Access Point alarm each minute the Access Point can be seen by a Sensor and is not selected as* ***Authorized*** *or* ***Ignore*** *in the AirDefense Policy Manager. For more information on Authorizing and Ignoring Access Points and Stations, see Chapter 5, Policy Manager.*



Steps to Use Rogue Summary

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK.**

4	Select a date from the date pick list and click **Load**	01/03/2003 Load

Rogue Summary displays the following:

Column	Displays...
Device	The color-coded icon and Device Identifier of the rogue Access Point or Station.
Sensor	The color-coded icon and Device Identifier of the Sensor that is detecting the rogue device.
Group	The Group ot which the Sensor belongs.
Location	The Location to which the Sensor belongs.
Last Alarm	The exact time and date of the last alarm generated by AirDefense.
Days Active	The number of days since the earliest unacknowledged alarm.

Note: Hovering your mouse over the Device or Sensor on the Rogue Summary displays detailed Device Identifier information.

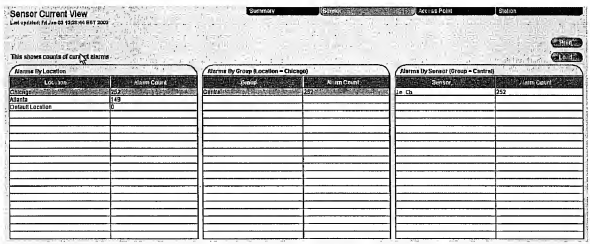
Click the Sensor tab to expand the pull-down for selecting Sensor reports. There are three possible reports--see the table below.

Sensor Report	This Report...
Sensor Current View	Shows you counts of alarms generated by Sensor, Group, and Location.
Sensor Channel View	Shows network statistics for each channel, filtered by Sensors. You may view which Access Points, Stations, or ad hoc networks were detected on specific channels, how many bytes of data were transmitted, and more
Sensor Performance View	Shows a daily overview of your network statistics per channel, based on selected Sensors

7.4.1 Sensor Current View

Sensor Current View displays the outstanding active alarms generated by individual Sensors. These are alarms that have not yet been cleared by your administrator. There are three separate displays on this page. They display active alarms by:

- Location
- Group
- Sensor



Steps to Use Sensor Current View

To use Sensor Current View, click **Load.** 

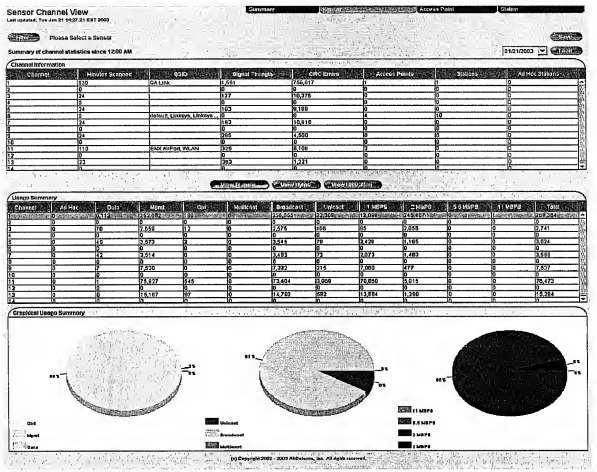
Sensor View displays the following:

Table	This Table...
Alarms by Location	Identifies all Locations you created in Sensor Manager (see "Configuring Locations, Groups, and Sensors" on page 67). The right-hand column displays a total number of outstanding active alarms generated by all Sensors belonging to that Location. Selecting a Location in this table changes the data displayed in the **Alarms by Group** screen.
Alarms by Group	Displays the names of each Group, showing the total number of outstanding active alarms within each Group. Selecting a Group within this table changes the data displayed in the **Alarms by Sensor** screen.
Alarms by Sensor	Displays the individual Sensors within the selected Group, and its total number of active alarms since the previous midnight.

7.4.2 Sensor Channel View

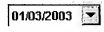
The Sensor Channel View screen provide information about network traffic for each channel AirDefense is monitoring.There are three displays:

- Channel Information
- Usage Summary
- Graphical Usage Summary

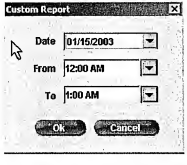


Steps to Use Sensor Channel View

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears.*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK.** ***Note:*** You may only view channel information on one Sensor at a time. Before you can load a report, you must first select a Sensor.)
4	.Select a date from the date pick list



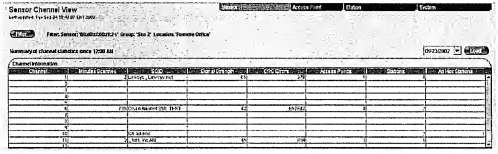
In addition to selecting a date, you may filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* **OK.**



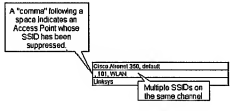
5	Click **Load.**

Channel Information

Channel Information displays information about network statistics for each channel scanned since midnight.



Channel Information displays the following

Column	Displays...
Channel	Numbers that represent the 14 channels AirDefense can scan. Data will only display in the table rows for the channels AirDefense actually scanned during the 24 hour period beginning at midnight.
Minutes Scanned	The total number of minutes over a 24 hour period that AirDefense monitored the particular channel.
SSID	The SSID detected on the channel. If more than one SSID is reported, it may indicate two or more Access Points are broadcasting on the same channel, which may negatively affect performance.  *Note:* Overlapping signals on the same channel potentially generate excessive CRC errors and loss of data.
Signal Strength	The average signal strength, since midnight, of all traffic on the specified channel.
CRC Errors	The total number of CRC errors detected, since midnight, while AirDefense monitored the channel.
Access Points	The total number of Access Points AirDefense detected on the channel since midnight.

Column	Displays...
Stations	The total number of Stations AirDefense detected on the channel since mid-night.
Ad Hoc Stations	The total number of Stations that AirDefense detected were operating in ad hoc mode.

Usage Summary

Usage Summary displays frame, byte, and utilization statistics about each channel the selected Sensor monitor. This is information on how much data is being transmitted on each channel in that segment of your WLAN.

Reading Usage Summary

Click **View Frames**, **View Bytes**, or **View Utilization** to change the type of data that displays.

- When viewing *frame data*, the numbers reflect the number of frames that were transmitted over the channel.
- When viewing *byte data*, the numbers reflect the number of bytes for each type of frame that were transmitted over the channel.
- When viewing *utilization data*, the report displays the percentage of total traffic each frame-type represented.

The table columns offer different ways to look at the data.

- The Data, Management, and Control columns represent parts of a whole: the "Data" column reports the actual data or payload frames, where the Control and Management columns report the smaller 802.11 frames (management and control frames, as opposed to data frames).
- The "Multicast, Broadcast, and Unicast columns are parts of a whole: Multicast frames use a protocol allowing anyone to listen to them, but individual Stations elect whether to receive them or not, Broadcastframes are sent to and received by all Stations, and Unicast frames are sent to and received by only one Station.
- The four Data Transfer Rate columns are parts of a whole: each shows how many frames or bytes were transmitted at their respective transfer rates.

Usage Summary displays the following information.

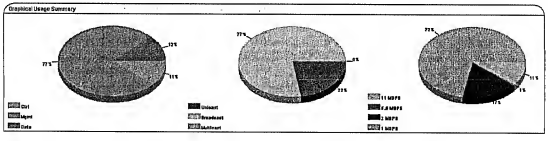
Column	Displays...
Channel	Numbers that represent the 14 channels AirDefense can scan. Data will only display in the table rows for the channel AirDefense actually scanned during the 24-hour period beginning at midnight. If data originating on adjacent channels bleeds over into the Channel the Sensor is monitoring, it is included here—giving you a true picture of how busy the channel is.
Ad Hoc	The total number of frames, bytes, or percentage of traffic (utilization) that were detected in ad hoc sessions.
Data	The total number of data frames, bytes, or the percentage of total traffic (utilization) they represented. (In utilization view, the numbers in this, and the Management and Control columns should add up to 100.)
Control	Reports the total number of control frames, bytes, or the percentage of total traffic (utilization) they represented. (In utilization view, the numbers in this, and the Data and Management columns should add up to 100.)
Management	The total number of management frames, bytes, or the percentage of total traffic (utilization) they represented. (In utilization view, the numbers in this, and the Data and Control columns should add up to 100.)
Multicast	The total number of multicast frames, bytes, or the percentage of traffic (utilization) they represented. (In utilization view, the numbers in this, and the Broadcast and Unicast columns should add up to 100.)
Broadcast	The total number of broadcast frames, bytes, or the percentage of traffic (utilization) they represented. (In utilization view, the numbers in this, and the Multicast and Unicast columns should add up to 100.)
Unicast	The total number of unicast frames, bytes, or the percentage of traffic (utilization) they represented. (In utilization view, the numbers in this, and the Multicast and Broadcast columns should add up to 100.)
1 Mbps	The total number of frames, bytes, or the percentage of traffic (utilization) transmitted at 1 MBPS. (In utilization view, the numbers in this, and the 2, 5.5 and 11 MBPS columns should add up to 100.)
2 Mbps	The total number of frames, bytes, or the percentage of traffic (utilization) transmitted at 2 MBPS. (In utilization view, the numbers in this, and the 1, 5.5 and 11 MBPS columns should add up to 100.)
5.5 Mbps	The total number of frames, bytes, or the percentage of traffic (utilization) transmitted at 5.5 MBPS. (In utilization view, the numbers in this, and the 1, 2 and 11 MBPS columns should add up to 100.)

Column	Displays...
11 Mbps	The total number of frames, bytes, or the percentage of traffic (utilization) transmitted at 11 MBPS. (In utilization view, the numbers in this, and the 1, 2 and 5.5 MBPS columns should add up to 100.)
Total	The total number of frames or bytes transmitted since midnight. (In "utilization view," this column reports "N/A"—i.e. does not apply.)

Graphical Usage Summary

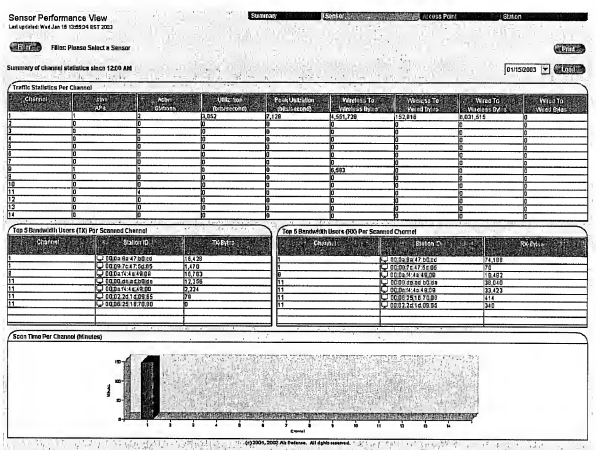
The **Graphical Usage Summary** charts graphically present three characteristics of your wireless traffic:

- Volume of Control, Management, and Data frames
- Volume of Multicast, Unicast, and Broadcast frames
- Volume of 1 MB/S, 2 MB/S, 5.5 MB/S, and 11 MB/S traffic.



7.4.3 Sensor Performance View

Sensor Performance View provides a daily overview of your network statistics per channel based on selected Sensors. This includes information about your network traffic, enabling you to identify over- and under-used Access Points, Stations, and assess bandwidth needs.

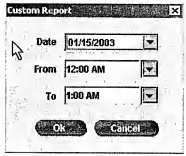


Steps to Use Sensor Performance View

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears.*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK**.

4	Select a date from the date pick list.

In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* **OK**.



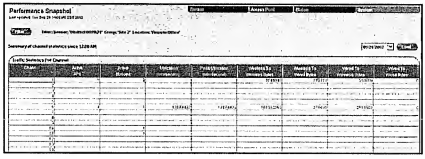
5	Click **Load**.

Four sets of data display:

- Traffic Statistics Per Channel
- Top 5 Bandwidth Users (TX) Per Scanned Channel
- Top 5 Bandwidth Users (RX) Per Scanned Channel
- Scan Time Per Channel (Minutes)

Traffic Statistics Per Channel

Traffic Statistics Per Channel displays more detailed information about the network statistics for each channel.

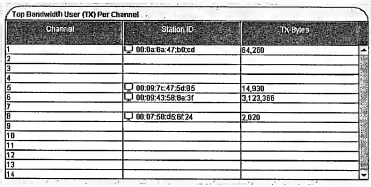


Traffic Statistics Per Channel table displays the following:

Column	Displays...
Channel Number	Numbers that represent the 14 channels AirDefense can scan. Data will only display in the table rows for the channel AirDefense actually scanned during the 24 hour period beginning at midnight.
Active APs	The number of Access Points heard transmitting and receiving on the specific channel.
Active Stations	The number of Stations heard transmitting and receiving on the specific channel.
Utilization (bits/second)	The average number of bits per second transmitted over the channel since midnight. ***Note:*** The average includes non-work hours—e.g., midnight to 8 AM and 6 PM to 11:59 PM. AirDefense takes the total bits transmitted in one minute and divides the number by 60 to generate the value displayed here.
Peak Utilization (bits/second)	The greatest number of bits per second transmitted in any minute since midnight. (AirDefense notes the one minute in a 24-hour period in which the most data was transmitted. It divides that number by 60 to produce the value displayed here.)
Wireless to Wireless Bytes	The total number of bytes transmitted within the wireless network.
Wireless to Wired Bytes	The total number of bytes transmitted from the wireless network to a wired segment of the network.
Wired to Wireless Bytes	The total number of bytes transmitted from the wired network to a wireless segment of the network.
Wired to Wired Bytes	The total number of bytes transmitted from the wired network to another segment of the wired network.

Top Bandwidth Users (TX) Per Scanned Channel

Top Bandwidth Users (TX) Per Channel Scanned displays the Stations that transmitted the most bytes of data per channel since midnight.

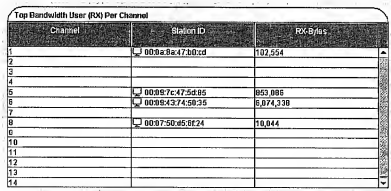


Top Bandwidth Users (TX) Per Scanned Channel displays the following:

Column	Displays...
Channel	The fourteen channels AirDefense can scan. The channel number indicates the channel the Station is transmitting data on during the 24 hour period beginning at midnight.
Station ID	The Device Identifier of the Station that is transmitting the data on the channel number indicated.
TX-Bytes	The total number of bytes each Station transmitted on the channel since midnight.

Top Bandwidth Users (RX) Per Scanned Channel

Top Bandwidth Users (RX) Per Scanned Channel identifies the Stations that received the most bytes of data per channel since midnight.



Top Bandwidth Users (RX) Per Scanned Channel displays the following

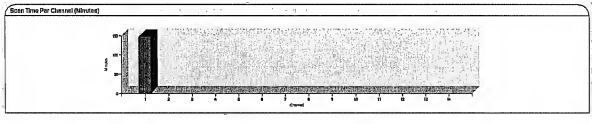
Column	Displays...
Channel	The fourteen channels AirDefense can scan. The channel number indicates the channel the Station is receiving data on during the 24 hour period beginning at midnight.
Station ID	The Device Identifier of the Station that is receiving the data on the channel number indicated.
RX-Bytes	The total number of bytes each Station received on the channel since midnight.

Scan Time Per Channel (Minutes)

A bar graph shows the total number of minutes during the 24-hour period that the Sensor listened on specific channels.

- **Vertical Y axis:** Displays minutes
- **Horizontal X axis:** Displays channels.

Rest your mouse over the bars to display a pop-out window showing the number of minutes



Click the Access Point tab to expand a sub-menu for selecting Access Point reports

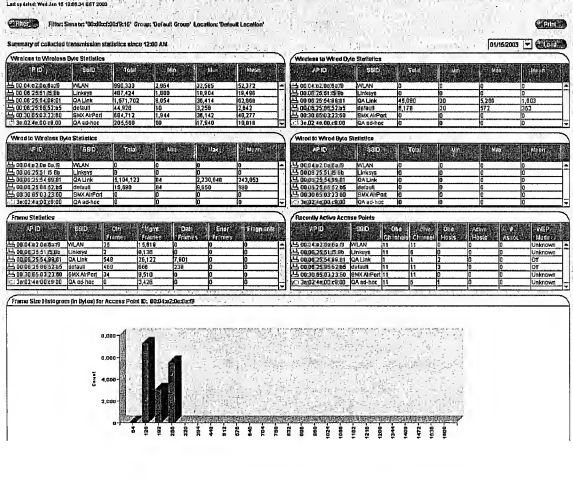
- **AP Summary:** Summarizes network traffic statistics for each Access Point.
- **AP Statistics:** Displays minute-by-minute network traffic statistics for each Access Point.
- **AP Policy Violations:** Displays statistics on Access Points that are in violation of policies.
- **Unauthorized APs:** Displays all Access Points and Stations are not authorized on the WLAN, by Group, Location, and Sensor.

7.5.1 AP Summary

The Access Point Summary provides a cumulative total, since midnight, of statistics about each Access Points' network activity.

A date pick list at the top right of the window allows you to view Access Point summaries for the previous 30 days.

> ***Note:*** In addition to selecting a date, you may filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** from the **Date** pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists.

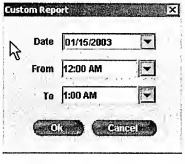


Steps to Use AP Summary

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears.*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK.**

4	Select a date from the date pick list.

In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* **OK.**



5	Click **Load.**

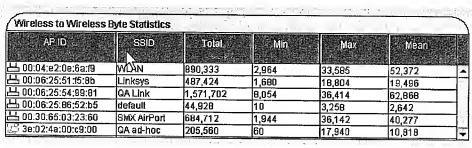
Note: When viewing the Access Point summary for the *current* day, the information displayed on this page is static—it is current up to the moment you click **Load.** To refresh the page (that is, include traffic statistics since the summary was last loaded in the browser window) click **Refresh or Load** again.

The summary displays:

- Wireless to Wireless Byte Statistics
- Wired to Wireless Byte Statistics
- Wireless to Wired Byte Statistics
- Wired to Wired Bye Statistics
- Frame Statistics
- Recently Active Access Points
- Frame Size Histogram

Wireless to Wireless Byte Statistics

Wireless to wireless bytes refer to bytes whose source and destination were inside the wireless network. Use this table to view which Access Point is handling the most wireless to wireless network traffic since midnight.



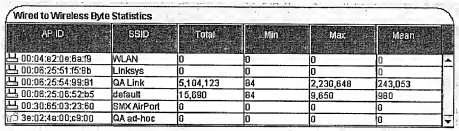
Wireless-to-Wireless Byte Statistics displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. ***Note:*** Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Total	The total number of bytes sent between wireless hosts since midnight.
Min	The minimum (smallest) number of bytes sent within any minute since midnight between wireless hosts.
Max	The maximum (largest) number of bytes sent within any minute since midnight between wireless hosts.

Column	Displays...
Mean	The mean number of bytes sent within any minute since midnight between wireless hosts.
Non-Zero Mean	The non-zero mean—the mean number of bytes just for those minutes when there was traffic. *Note:* There are times when *no data* is being transmitted. This provides a "truer" mean reflecting only the periods when there was network activity. The fact that minimum, maximum, and mean values use different time frames warrants additional comment. The "mean" value should never be higher than the maximum, but may be less than the minimum. You may sometimes see that a mean value is lower than the minimum or higher than the maximum value, which on first appearance doesn't make sense. This is because the mean value is looking at *all* the minute-by-minute values since midnight, while the minimum and maximum values are only showing the transmission for a *single* minute. Additionally, if you have a workstation that transmitted several large files during a twenty-minute period in the day, but was otherwise inactive, the mean value might be significantly less meaningful than the non-zero mean. The non-zero mean will show the mean only for those minutes in which data was actually transmitted or received.

Wired to Wireless Byte Statistics

Wired to wireless bytes refer to bytes that originated on a physical segment of the network, but whose destination was inside the wireless network. Use this table to view which Access Point is handling the most wired to wireless network traffic since midnight.



Wired to Wireless Byte Statistics

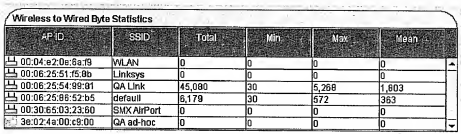
AP ID	SSID	Total	Min	Max	Mean
00:04:e2:0e:8a:f9	WLAN	0	0	0	0
00:06:25:51:f5:9b	Linksys	0	0	0	0
00:06:25:54:99:81	QA Link	5,104,123	64	2,230,648	243,053
00:08:25:06:52:b5	default	15,090	64	9,650	980
00:30:65:03:23:60	SMX AirPort	0	0	0	0
3e:02:4a:00:c9:00	QA ad-hoc	0	0	0	0

Wired-to-Wireless Byte Statistics displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. ***Note:*** Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Total	The total number of bytes sent from wired hosts to wireless Stations since midnight.
Min	The minimum (smallest) number of bytes sent within any minute since midnight from wired hosts to wireless Stations.
Max	The maximum (largest) number of bytes sent within any minute since midnight from wired hosts to wireless Stations.
Mean	The mean number of bytes sent from wired hosts to wireless Stations since midnight.
Non-Zero Mean	The non-zero mean—the mean number of bytes just for those minutes when there was traffic (because there are times when no data is transmitting). This provides a "truer" mean reflecting only the periods when there was network activity.

Wireless to Wired Byte Statistics

Wireless to wired bytes refer to bytes that originated inside the wireless network, but whose destination was on a *physical* segment of the network. Use this table to view which Access Point is handling the most wireless to wired network traffic since midnight.



Wireless to Wired Byte Statistics

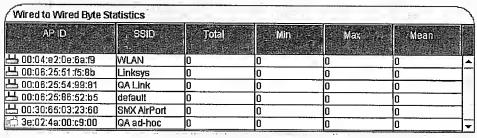
AP ID	SSID	Total	Min	Max	Mean
00:04:e2:0e:8a:f9	WLAN	0	0	0	0
00:06:25:51:f5:8b	Linksys	0	0	0	0
00:06:25:54:99:81	QA Link	45,080	30	5,268	1,803
00:06:25:86:52:b5	default	6,179	30	572	363
00:30:65:03:23:60	SMX AirPort	0	0	0	0
3e:02:4e:00:c9:00	QA ad-hoc	0	0	0	0

The Wired-to-Wireless Byte Statistics table displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. ***Note:*** Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Total	The total number of bytes sent from wireless Stations to wired hosts since midnight.
Min	The minimum (smallest) number of bytes sent within any minute since midnight from wireless Stations to wired hosts.
Max	The maximum (largest) number of bytes sent within any minute since midnight from wireless Stations to wired hosts.
Mean	The mean number of bytes sent from wireless Stations to wired hosts since midnight.
Non-Zero Mean	The non-zero mean—the mean number of bytes just for those minutes when there was traffic (because there are times when *no data* is transmitting). This provides a "truer" mean reflecting only the periods when there was network activity.

Wired to Wired Byte Statistics

Wired to wired bytes refer to bytes whose source and destination were both on a *physical* segment of the network but traversed the wireless network. Use this table to view which Access Point is handling the most wired to wired (bridged) network traffic since midnight.


Wired to Wired Byte Statistics

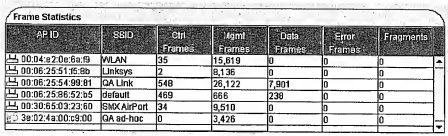
AP ID	SSID	Total	Min	Max	Mean
00:04:e2:0e:8a:f9	WLAN	0	0	0	0
00:06:25:51:f5:8b	Linksys	0	0	0	0
00:06:25:54:99:81	QA Link	0	0	0	0
00:06:25:86:52:b5	default	0	0	0	0
00:30:65:03:23:60	SMX AirPort	0	0	0	0
3e:02:4a:00:c9:00	QA ad-hoc	0	0	0	0

Wired-to-Wired Byte Statistics displays the following information.

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. ***Note:*** Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Total	The total number of bytes sent from wired hosts to wired hosts since midnight.
Min	The minimum (smallest) number of bytes sent within any minute since midnight from wired hosts to wired hosts.
Max	The maximum (largest) number of bytes sent within any minute since midnight from wired hosts to wired hosts.
Mean	The mean number of bytes sent from wired hosts to wired hosts since midnight.
Non-Zero Mean	The non-zero mean—the mean number of bytes just for those minutes when there was traffic (because there are times when *no data* is transmitting). This provides a "truer" mean reflecting only the periods when there was network activity.

Frame Statistics

AirDefense gives you an overview of each Access Point's frame statistics, since midnight, whose data might help you identify network configuration issues or possible intrusion attempts.



Frame Statistics displays the following:

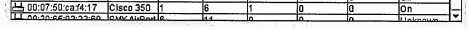
Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. *Note:* Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Ctrl Frames	The number of control frames transmitted to or received by the Access Point since midnight. (Control frames carry the data that negotiate the 802.11 protocol for getting the data onto the airwaves.)
Mgmt Frames	The number of management frames transmitted to or received by the Access Point since midnight. (Management frames carry the data that negotiate network connections.)
Data Frames	The number of data frames transmitted to or received by the Access Point since midnight. Very high numbers indicate large file transfers. (Data frames carry the "payload"—the actual data.)

Column	Displays...
Error Frames	The number of error frames transmitted to or received by the Access Point since midnight. (Error frames result when frames become corrupted—due to a variety of factors—and the frame's data no longer matches the CRC. Unusually large numbers of Error frames indicate that an attacker is flooding your WLAN with frames designed to damage your wireless traffic, or that other significant problems are affecting WLAN performance.)
Fragments	The number of fragment frames detected since midnight. (If there are an exceptionally high number of fragments, it may indicate that your network is not configured optimally—too many packets are being split up due to their being routed to mismatched hardware. Alternately, it may indicate a "buffer overflow-type" attack in which a hacker is hoping to cripple your network by flooding it with incomplete packets.) ***Note:*** Fragment frames are the result of Layer 1 of the 802.11b protocol separating large amounts of data into "pieces" small enough to put out on the air.

Recently Active Access Points

AirDefense monitors additional statistics about your BSSs. The information shown here may reveal outside attempts to break into the wireless network. Unlike the other five tables on this page that show a *summary* of data since midnight, this table shows a minute-by-minute display of detected Access Points. That is, the table is updated each minute to display information detected in the previous minute.

Note: Since this is the most recent minute, if the date prior to today's or a custom time (not including the last minute) is selected, the table will be empty.

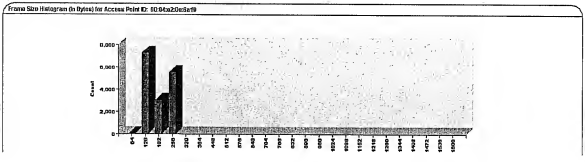


Recently Active Access Points displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The SSID of the Access Point. ***Note:*** Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs (SSIDs). Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set are in physical proximity to each other. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, they must broadcast a probe request announcing the Extended Service Set they wish to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Obs Channels	The total number of channels on which the Access Point was detected since midnight.
Active Channel	The Access Point's *current* active channel (i.e. in the past minute). If this channel ever varies from your initial configuration, it may indicate mis-configuration, or possible attempts at Access Point identity theft.
Obs Hosts	How many Stations have been observed sending or receiving network frames through a specific Access Point since midnight.
Active Hosts	How many Stations were *currently* associated with an Access Point and sending and receiving frames in the past minute.
# Assoc	How many times Stations have associated with the Access Point during the previous minute.
WEP Mode	Whether the Access Point used Wired Equivalent Privacy (WEP) in the past minute. • **Off:** WEP was off. • **On:** WEP was on. • **Both:** WEP was configured for both (AirDefense ignores state). • **Unknown:** (Stations only).

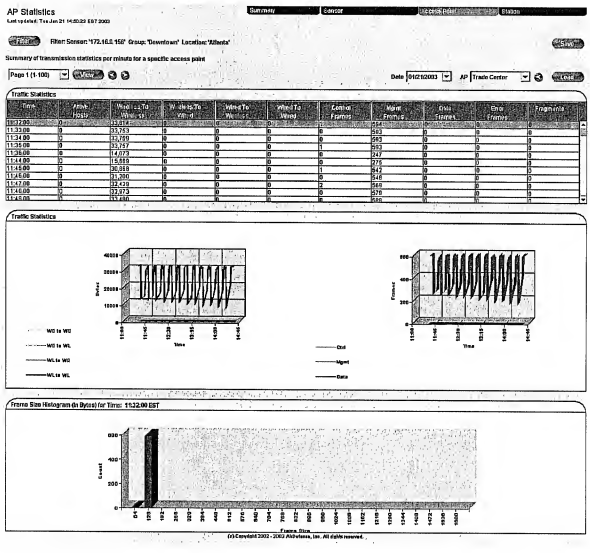
Frame Size Histogram in Bytes

A Frame Size Histogram at the bottom of the window shows a graphical report of how many frames of specific sizes were transmitted since midnight by the selected Access Point. (Select an Access Point in any table on this page to view its Frame Size Histogram of network traffic since midnight—the title of the histogram displays the Device Identifier of the Access Point.) Resting your mouse over each frame-size bar briefly displays the number of packets of that size that were observed. In the example shown below, there were six 64 byte frames, one thousand five 128 byte frames, eighty-seven 192 byte frames, one 256 byte frames, and nine 320 byte frames transmitted since midnight.



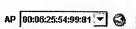
7.5.2 AP Statistics

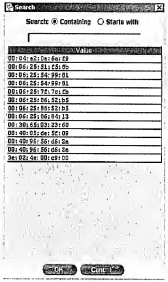
The Access Point Statistics report displays a minute-by-minute report of network activity for each configured Access Point. Use this Report to see detailed information about your Access Points' frame traffic to various nodes in your WLAN.



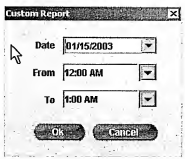
Steps to Use AP Statistics

Step	Action
1	Click Filter to select the Sensor that monitors the Access Point you want to view. *A Choose Filter Set screen appears.*
2	Click a Sensor in the screen.
3	Click **OK**.
4	Select a date from the AP (Access Point) pull-down list. Alternately, you can click on the arrow on the pull-down. A Search screen appears. Choose from the list on the Search screen, or conduct a search for a know Access Point.
5	Select a date from the date pick list.



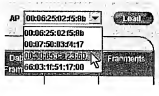


In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* ***OK****.*

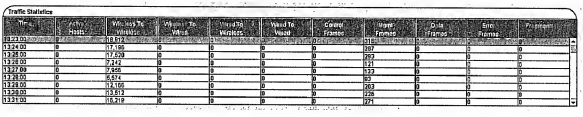


6 Click **Load.** This loads the Traffic Statistics page with data.

Note: (Resting your mouse over an Access Point's Device Identifier pops up a window that identifies the SSID to which it belongs.).



Traffic Statistics



Traffic Statistics displays the following:

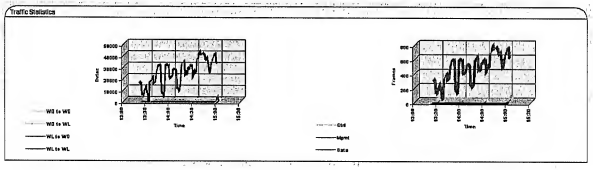
Column	Displays...
Time	The minute during which the network traffic data was collected.
Active Hosts	How many Stations were associated with the Access Point in the given minute.
Wireless to Wireless	How many bytes of data were transmitted and received between wireless Stations in that minute.
Wireless to Wired	How many bytes of data were transmitted from wireless Stations to the physical network in that minute.
Wired to Wireless	How many bytes of data were transmitted from the physical network to wireless Stations in that minute.
Wired to Wired	How many bytes of data were transmitted and received between one segment of the physical network through the WLAN to another segment of the physical network in that minute.
Control Frames	The total number of control frames transmitted and received in that minute.
Mgmt Frames	The total number of management frames transmitted and received in that minute.

Column	Displays...
Data Frames	The total number of data frames transmitted and received in that minute.
Error Frames	The total number of error frames transmitted and received in that minute.
Fragments	The total number of fragment frames transmitted and received in that minute.

Each page of traffic statistics contains up to 100 rows or minutes of data. To view data on additional pages, select the page from the **Page** pick list and click **View**, or click the left and right browse buttons. Any column of data may be sorted by clicking on a column heading.

Graphical Representation of Traffic Statistics

Immediately below the **Traffic Statistics** table is a graphical representation of the numeric data in the Traffic Statistics columns.

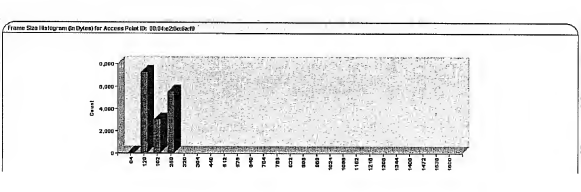


The Graphical Representation displays the following:

Element	Description
Left Block	Plots the transmission of bytes in your WLAN. The four directions of traffic are color-coded • **Light Blue:** Wired to Wired (WD to WD) traffic • **Green:** Wired to Wireless (WD to WL) • **Red:** Wireless to Wired (WL to WD) • **Dark Blue:** Wireless to Wireless (WL to WL) Axis Representations: • **Vertical Y Axis:** The number of bytes transmitted. • **Horizontal X Axis:** time. *Note:* Resting your mouse over areas of the graph popup a display of the number of bytes of data transmitted during that minute. This graphic may display regular, sharp spikes down to zero, if the Sensor is scanning multiple channels, and hears no data while listening on other channels.
Right Block	Plots the number of frames of each type that were sent over time. • **Green:** Control (Ctrl) frames • **Red:** Management (Mgmt) frames • **Blue:** Data frames Axis Representations: • **Vertical Y Axis:** The number of bytes transmitted. • **Horizontal X Axis:** time. Resting your mouse over areas of the graph popup a display of the number of bytes of data transmitted during that minute. This graphic may display regular, sharp spikes down to zero, if the Sensor is scanning multiple channels, and hears no data while listening on other channels.

Frame Size Histogram

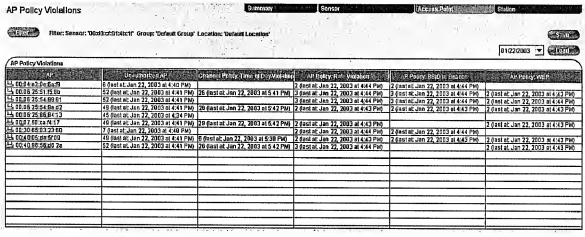
A Frame Size Histogram at the bottom of the window shows a graphical report of how many frames of specific sizes were transmitted each minute. Selecting a minute row in the **Traffic Statistics** table above displays the histogram for that minute (the histogram title shows the minute that is displayed). Resting your mouse over each frame-size bar briefly displays the number of packets of that size that were transmitted in that minute.



7.5.3 AP Policy Violations

AP Policy Violations displays statistics on Access Points that are having policy violations.

The first column that displays is always the Access Point color-coded icon and Device Identifier where policy violations are occuring. There is a varying number of secondary columns. The violations in the secondary columns coincide with the policy configurations for Access Points and Stations in Policy Manager (see "Create Policy: Configuration" on page 99 for descriptions of policy configurations).



AP Policy Violations displays the following:

Column	Displays...
AP	The color-coded icon and the device identifiers of the Access Points that are experiencing policy violations.
Unauthorized AP	The number of unauthorized AP policy violations that have occurred, and the time of the last occurrence of the violation. Unauthorized APs are Access Points that are not authorized for use in your WLAN.
Unauthorized Station	The number of unauthorized Station policy violations that have occurred, and the time of the last occurrence of the violation. Unauthorized Stations are those Stations that are not authorized for use with their associated Access Point.
AP Policy:WEP	The number of WEP policy violations that have occurred on the Access Point, and the time of the last occurence of the violation.
AP Policy: SSID in Beacon	The number of SSID in Beacon policy violations that have occurred on the Access Point, and the time of the last occurence of the violation.
AP Rate Violation	The number of Rate policy violations that have occurred on the Access Point, and the time of the last occurence of the violation.

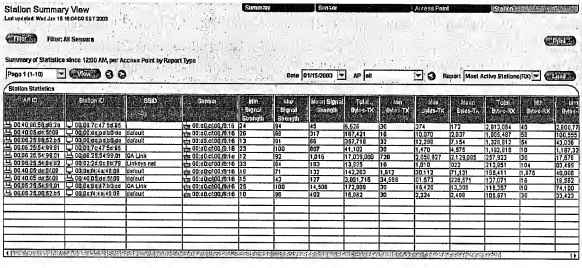
Column	Displays...
AP Policy: Auth Mode Violation	The number of Authentication Mode policy violations that have occurred on the Access Point, and the time of the last occurence of the violation
AP Policy: Channel	The number of Channel policy violations that have occurred on the Access Point, and the time of the last occurence of the violation.

Click the Station tab to expand a sub-menu for selecting Station reports. There are three possible reports:

- **Station Summary View:** This report shows summaries of network traffic statistics for each Station.
- **Station Current View:** This report shows network traffic statistics for each station for the most recent minute.
- **Single Station View:** This report shows minute-by-minute network traffic statistics a single Station.
- **Probing Stations:**This report shows

7.6.1 Station Summary View

The Station Summary View displays cumulative statistics about the transmissions of all Stations associated with each Access Point. Use this Report to determine ranges and thresholds for normal network traffic for each Station in your various BSSs.



Steps to Use Station Summary View

Note: Single-clicking on a Station immediately takes you to the **Single Station View** report where you may see a minute-by-minute breakdown of statistics for that Station (see "Single Station View" on page 209).

StepAction

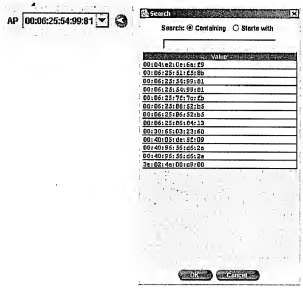
1Click **Filter** to select the Sensor that monitors the Access Points, that monitors the Stations for which you want to view statistics.

A Choose Filter Set screen appears.

2Click a Sensor in the screen.

3Click **OK.**

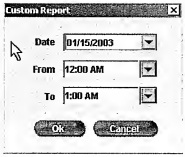
Select an AP (Access Point) from the AP pull-down list. Alternately, you can click on the arrow on the pull-down. A Search screen appears. Choose from the list on the Search screen, or conduct a search for a known Access Point.This must be the Access Point for which you want to view Station statistics.



Additional Device Identifiers for the Access Point display when the mouse rests over its Device Identifier.

5 Select a date from the date pick list.

In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* **OK.**



6 Click on one of four reports to display.

- **Most Active Stations (RX)**—the 10 most active *receiving* Stations
- **Most Active Stations (TX)**—the 10 most active *transmitting* Stations
- **Observed Stations**—*all* Stations observed communicating with the selected Access Point
- **New Stations**—Stations observed *today* that AirDefense *has never seen before.*

7 Click **Load.** This loads Station Summary View with data.

Note: (If there is more data than can fit on a page, additional pages are created.

To view data on additional pages, select the page from the **Page** *pick list and click* **View**, *or click the left and right browse buttons.) Any column of data may be sorted by clicking on a column heading.*

AirDefense Reporting

AirDefense reports the Device Identifiers both for Stations transmitting and receiving data on the WLAN, and Stations on the wired side of the network with whom they are transmitting or receiving data. For example, wireless Stations browsing the Internet will cause the network firewall's MAC address to be detected and displayed. AirDefense also reports any AirDefense Server or Station on the wired network that is being browsed by wireless users.

The four reports use the same screen to display their Station data. Because so much data displays, you must use the horizontal scroll bar at the bottom of the page to view the data on the right side of the table.

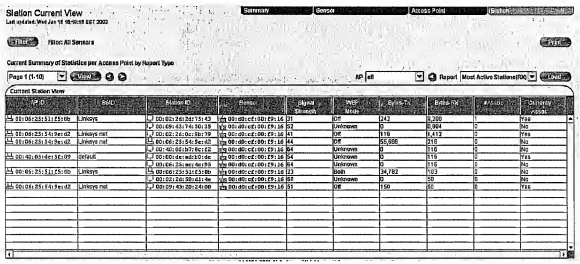
Station Summary View displays the following information.

Column	Displays...
AP ID	The MAC address of the Access Point the Station was associated with. (If a Station associates with another Access Point and meets the criteria of one of the reports, it will show up as an additional entry in this table, and its association with the other Access Point will be reported.)
Station ID	The Device Identifier of the reported Stations.
SSID	The name of the Extended Service Set, only if it can be determined.
Sensor	The name of the Sensor given it in the Sensor program area. If you did not provide a name for the Sensor, its IP address is listed instead.
Min Signal Strength	The minimum signal strength the Station experienced since midnight. (AirDefense observes and records the lowest signal strength for each minute throughout the day and displays the lowest value for that day.)
Max Signal Strength	The maximum signal strength the Station experienced since midnight. (AirDefense observes and records the highest signal strength for each minute throughout the day displays the highest value for that day.)
Mean Signal Strength	The mean signal strength the Station experienced *since midnight*.
Non-Zero Mean Signal Strength	The mean signal strength only for those times when the signal strength was not zero. ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero signal strength. This provides a truer mean signal strength. For a further description of non-zero means, see "Wireless to Wireless Byte Statistics" on page 185.
Total Bytes-RX	The total bytes of data received by the Station *since midnight*.
Min Bytes-RX	The minimum bytes of data received in any one minute period by the Station *since midnight*.
Max Bytes-RX	The maximum bytes of data received in any one minute period by the Station *since midnight*.
Mean Bytes-RX	The mean bytes per minute received by the Station *since midnight*. (AirDefense observes and records once a minute throughout the day both the high and low bytes transmitted, and automatically reports the mean.)
Non-Zero Mean Bytes-RX	The mean bytes received only for those minutes when received bytes was not zero. This provides a truer mean bytes. ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero bytes. This provides a "truer" mean bytes.

Column	Displays...
Total Bytes-TX	The total bytes of data transmitted by the Station *since midnight*.
Min Bytes-TX	The minimum bytes of data transmitted in any one minute period by the Station *since midnight*.
Max Bytes-TX	The maximum bytes of data transmitted in any one minute period by the Station *since midnight*.
Mean Bytes-TX	The mean bytes per minute transmitted by the Station *since midnight*. (AirDefense observes and records once a minute throughout the day both the high and low bytes transmitted, and automatically reports the mean.)
Non-Zero Mean Bytes-TX	The mean bytes transmitted only for those minutes when transmitted bytes was not "zero." ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero bytes.
# Assoc	The total number of associations to the Access Point each Station made since midnight. Ordinarily, this number should be low (< 3). High numbers are indicative of excessive logging on and off, attacks, or possible hardware or software failure.

7.6.2 Station Current View

The Station Current View page displays the traffic statistics that occurred in the last minute for each Access Point in the Basic Service Set. Use this report to view up-to-the-minute statistics about your current WLAN traffic.



Steps for Using Station Current View

Step **Action**

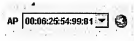
1 Click **Filter** to select the Sensor that monitors the Access Points, that monitors the Stations for which you want to view statistics.

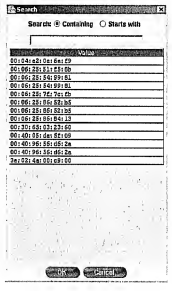
A Choose Filter Set screen appears.

2 Click a Sensor in the screen.

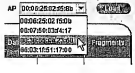
3 Click **OK.**

Select an AP (Access Point) from the AP pull-down list. Alternately, you can click on the arrow on the pull-down. A Search screen appears. Choose from the list on the Search screen, or conduct a search for a know Access Point.This must be the Access Point for which you want to view Station statistics.





Additional Device Identifiers for the Access Point display when the mouse rests over its Device Identifier.



5 Click on one of four reports to display.

- **Most Active Stations (RX)**—the 10 most active receiving Stations
- **Most Active Stations (TX)**—the 10 most active transmitting Stations
- **Observed Stations—all** Stations observed communicating with the selected Access Point
- **New Stations**—Stations observed today that AirDefense has never seen before.

6 Click **Load.** This loads Station Current View with data.

Note: (If there is more data than can fit on a page, additional pages are created.

To view data on additional pages, select the page from the **Page** *pick list and click* **View**, *or click the left and right browse buttons.) Any column of data may be sorted by clicking on a column heading*

Clicking on a Station takes you to the Single Station View report for that Station.

The four reports use the same table to display their network data. Because so much data is displayed, you must use the horizontal scroll bar at the bottom of the page to view the data on the right side of the table.

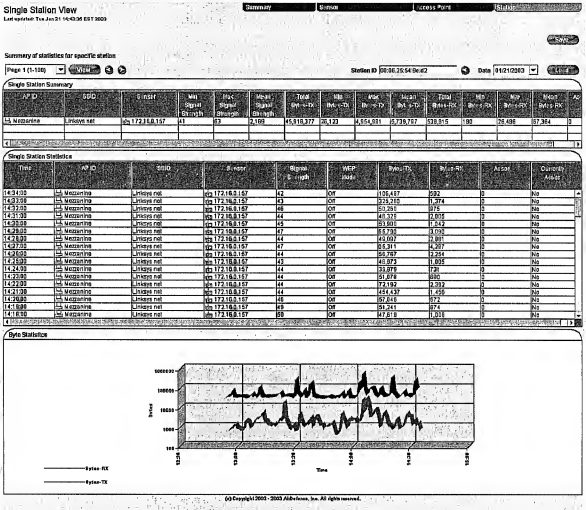
Station Current View screen displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point the Station is currently associated with.
Station ID	The Device Identifier of the reported Stations.
SSID	The name of the Extended Service Set, if it can be determined.
Sensor	The name of the Sensor given it in the Sensor program area. If you did not provide a name for the Sensor, its IP address is listed instead.
WEP Mode	The workstation's Wired Equivalent Privacy (WEP) status for the previous minute. • **Off:** WEP was off. • **On:** WEP was on. • **Both:** WEP was configured for both (AirDefense ignores state). • Unknown: (Stations only).
Signal Strength	The mean signal strength the Station experienced *during the minute*.
Bytes-RX	The total bytes of data received by the Station *during the minute*.
Bytes-TX	The total bytes of data transmitted by the Station *during the previous minute*.
Non-Zero Mean Bytes-TX	The mean bytes transmitted *since midnight* only for those portions of the minute when transmitted bytes was not zero. *Note:* There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero signal strength. This provides a truer mean bytes.

Column	Displays...
# Assoc	The total number of associations to the Access Point each Station made in the previous minute. Ordinarily, this number should be zero—it is expected that the Stations will have associated at some previous time. Any value higher than "1" is indicative of excessive logging on and off, movement of a portable Station, attacks, or hardware/software failure.
Currently Assoc	• **Yes:** At the end of the previous minute, the Station was currently associated with an Access Point • **No:** At the end of the previous minute, the Station was NOT currently associated with an Access Point.

7.6.3 Single Station View

The Single Station View displays minute-by-minute transmission statistics for individual Stations. Use this Report to view a history of each individual Station's network traffic.



Steps to Use Single Station View

Note: Clicking a Station in the **Station Summary** or **Station Current View** report will also open this report and load the table with data.

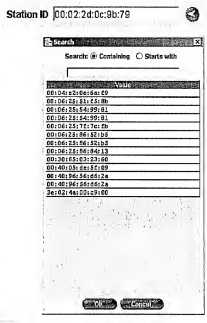
Step	Action
1	Select a Station from the Station ID pull-down list.

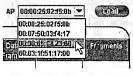
Alternately, you can click on the arrow on the pull-down.

A Search screen appears.

Choose from the list on the Search screen, or conduct a search for a know Station. This must be the Station for which you want to view Station statistics.

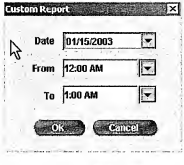
Additional Device Identifiers for the Access Point display when the mouse rests over its Device Identifier.





2	Select a date from the date pick list.

In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* ***OK****.*



3	Click **Load**. This loads Single Station View with data.

Note: (If there is more data than can fit on a page, additional pages are created.

To view data on additional pages, select the page from the **Page** *pick list and click* **View,** *or click the left and right browse buttons.) Any column of data may be sorted by clicking on a column heading.*

Single Station Summary

The **Single Station Summary** table provides a summary of network traffic between the Station and each Access Point it was associated with since midnight.

The Single Station View screen displays the following:

Column	Displays...
AP ID	The Device Identifier of the Access Point.
SSID	The name of the Extended Service Set, if it can be determined.
Sensor	The name of the Sensor given it in the Sensor program area. If you did not provide a name for the Sensor, its IP address is listed instead.
Min Signal Strength	The minimum signal strength the Station experienced since midnight. (AirDefense observes and records the lowest signal strength for each minute throughout the day and displays the lowest value.)
Max Signal Strength	The maximum signal strength the Station experienced since midnight. (AirDefense observes and records the highest signal strength for each minute throughout the day displays the highest value.)
Mean Signal Strength	The mean signal strength the Station experienced *since midnight.*
Non-Zero Mean Signal Strength	The mean signal strength only for those times when the signal strength was not zero. ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as "zero signal strength.This provides a truer mean signal strength. For a further description of non-zero means, see "Wireless to Wireless Byte Statistics" on page 185.
Total Bytes-RX	The total bytes of data received by the Station *since midnight.*
Min Bytes-RX	The minimum bytes of data received in any one minute period by the Station *since midnight.*
Max Bytes-RX	The maximum bytes of data received in any one minute period by the Station *since midnight.*
Mean Bytes-RX	The mean bytes per minute received by the Station *since midnight.* (AirDefense observes and records once a minute throughout the day both the high and low bytes transmitted, and automatically reports the mean.)

Column	Displays...
Non-Zero Mean Bytes-RX	The mean bytes received only for those minutes when received bytes was not zero. ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero bytes. This provides a truer mean bytes.
Total Bytes-TX	The total bytes of data transmitted by the Station *since midnight.*
Min Bytes-TX	The minimum bytes of data transmitted in any one minute period by the Station *since midnight.*
Max Bytes-TX	The maximum bytes of data transmitted in any one minute period by the Station *since midnight.*
Mean Bytes-TX	The mean bytes per minute transmitted by the Station *since midnight.* (AirDefense observes and records once a minute throughout the day both the high and low bytes transmitted, and automatically reports the mean.)
Non-Zero Mean Bytes-TX	The mean bytes transmitted only for those minutes when transmitted bytes was not zero. ***Note:*** There are many times throughout the day when the Station is neither sending nor receiving. AirDefense interprets these periods of silence as zero bytes. This provides a truer mean bytes.
Assoc	The total number of associations to the Access Point the Station made since midnight. Ordinarily, this number should be low (< 3). High numbers are indicative of excessive logging on and off, attacks, or possible hardware or software failure.

Single Station Statistics

Each row in the table reflects one minute of activity. (The first row in the report displays a summary of data collected over the past thirty days for that Station.) If the report contains more data than can fit on a page—100 rows of data—additional pages are created.

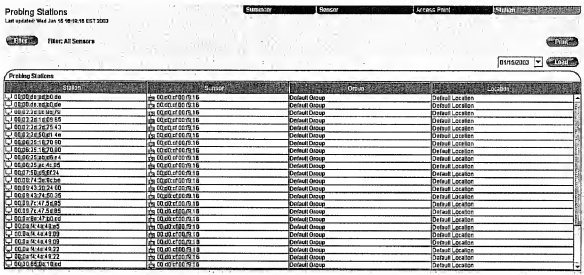
To view data on additional pages, select the page from the **Page** *pick list and click* **View**, *or click the left and right browse buttons.) Any column of data may be sorted by clicking on a column heading.* Because so much data is displayed, you must use the horizontal scroll bar at the bottom of the page to view the data on the right side of the table.

Single Station Statistics displays the following:

Column	Displays...
Time	The minute for which the data was recorded.
AP ID	The Device Identifier of the Access Point the Station was associated with during the specified minute.
SSID	The name of the Extended Service Set, if it can be determined.
Sensor	The name of the Sensor given it in the Sensor program area. If you did not provide a name for the Sensor, its IP address is listed instead.
Signal Strength	The mean signal strength that AirDefense detected *since midnight*. ***Note:*** You may notice what appears to be a disparity between the Mean Signal Strength in the **Single Station Summary** table and the minute-by-minute Signal Strength reported here in the **Single Station Statistics** table. This may be because the Mean Signal Strength is calculated over the 24-hour period since midnight, and will include times when the Station moved to another location, or became inactive for a period of time. And if the Sensor was scanning multiple channels, by definition it will not be listening to that Station's network traffic while it is on another channel, and that time will be calculated as zero-signal strength, bringing the mean signal strength value down. To find the mean signal strength for the minutes when the Station was actually active, scroll through the pages of data (using the **View** and page browse buttons) to find the begin and end times of activity. Then filter your view of the data by creating a custom date filter using the Date pick list and the begin and end time you discovered within the pages.
WEP Mode	The Station's Wired Equivalent Privacy (WEP) status in a given minute. • **Off:** WEP was off. • **On:** WEP was on. • **Both:** WEP was configured for both (AirDefense ignores state). • **Unknown:** (Stations only).
Bytes-RX	The total bytes of data received by the Station *since midnight*.
Bytes-TX	The total bytes of data transmitted by the Station *since midnight*.
# Assoc	The total number of associations to the Access Point the Station made in that minute. Ordinarily, this number should be zero—it is expected that the Stations will have associated at some previous time. Any value higher than 1 is indicative of excessive logging on and off, attacks, or hardware/software failure.
Currently Assoc	• **Yes:** At the end of a given minute, the Station was currently associated with an Access Point. • **No:** At the end of a given minute, the Station was currently NOT associated with an Access Point. ***Note:*** Variable Yes' and No's may indicate a Station is mobile—moving in and out of an Access Point's "air space."

7.6.4 Probing Stations

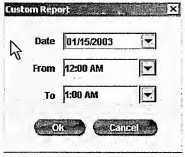
Use Probing Stations to view which Stations are being subjected to reconnaissance activities, possibly for attack.



Steps to Use Probing Stations

Step	Action
1	Click **Filter** to limit the reports to a specific Location, Group, or Sensor. *A Choose Filter Set screen appears.*
2	Click a Location, Group, or Sensor in the screen.
3	Click **OK.**
4	Select a date from the date pick list.

In addition to selecting a date, you can filter the data by specifying a select range of hours whose data you want to view. Select **Custom...** *from the* **Date** *pick list. In the resulting date window, select a date, and a start hour and end hour, in the available pick lists. Click* ***OK.***



5 Click **Load.** 

Probing Stations displays the following information.

Column	Displays...
Station	The color-coded icon and Device Identifier of the Station being subjected to a probe.
Sensor	The color-coded icon and Device Identifier of the Sensor that is detecting the probe.
Group	The color-coded icon and Device Identifier of the Sensor's Group.
Location	The color-coded icon and Device Identifier of the Sensor's Location.

8 Administration

Use Administration to do the following:

- Provide AirDefense with user name, role, and password information
- Configure your display preference
- Export and backup data
- Update the AirDefense software
- Request and install security certificates
- Name your AirDefense system

AirDefense provides you with the ability to export a variety of data for archival and forensic purposes. It also provides an interface for requesting and installing a Security Certificate on the AirDefense Server so that users can administer the AirDefense application securely over an encrypted https web session.

8.0.1 In This Chapter

This chapter contains the following topics.

User Info

Use the User Information tables to do the following:

- View the current user and current role (for example, Administrator)
- Change the password of the current user
- Change the password of any user on AirDefense
- Add a user to AirDefense
- Delete a user from AirDefense

The Role of the User

You can assign user access according to the roles of individuals in your organization. Individuals can be a guest with read-only privileges, or they can be an administrator, with both read and write privileges.

Administrators:

The default user for AirDefense is **smxmgr**--the root user (administrator). The administrator can add new users to AirDefense and can assign them to a role, *including as another administrator.* An individual with administration privileges (**Admin**) can change configurations throughout the database.Only administrators can change configurations throughout AirDefense, such as changing policies or authorizing Access Points and Stations.

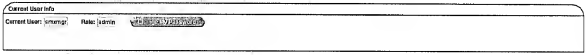
Guests:

A guest user can only view data, i.e., monitor the various states in the AirDefense. ***A guest will only be able to see the User Info and User Preferences portions of Administration.***

8.1.1 Current User Information

The Current User table displays the current user and their role. You can use this table to change the password of the current user.

Note: The default user is smxmgr. This is the root user (administrator) of AirDefense.

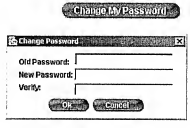


The table below describes the fields in the Current User table.

Field	Meaning
Current User	Displays the current user. (AirDefense default is **smxmgr**.)
Role	Displays the user-assigned role of the current user, for example, Administrator.

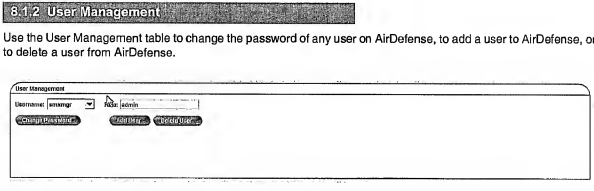
Steps to Change the Password of the Current User

Step	Action
1	Click **Change My Password**. *The Change Password screen appears.*
2	Enter your old password on the Change Password screen, followed by your new password.
3	Enter your new password again to verify.
4	Click **OK** to save, or **Cancel** to cancel.



8.1.2 User Management

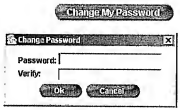
Use the User Management table to change the password of any user on AirDefense, to add a user to AirDefense, or to delete a user from AirDefense.



Field	Meaning
User Name	This pull-down lists every user currently authorized to use AirDefense.
Role	This field displays the role of the user that currently displays in the Use Name window.

Steps to Change the Password of Any User

Step	Action
1	Click **Change My Password**. *The Change Password screen appears.*
2	Enter your new password on the Change Password screen.
3	Enter your new password to verify.
4	Click **OK** to save, or **Cancel** to cancel.

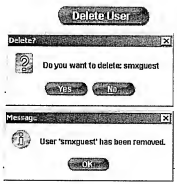


Steps to Add a User to AirDefense

Step	Action
1	Click **Change My Password**. *The Change Password screen appears.*
2	Enter your new password on the Change Password screen.
3	Enter your new password to verify.
4	Click **OK** to save, or **Cancel** to cancel.

Steps to Delete a User from AirDefense

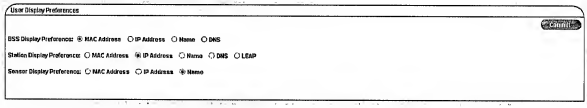
Step	Action
1	Click **Delete User**. *The Delete? screen appears.*
2	Click **YES** to delete. *A confirmation Message screen appears.* *Alternately, click **NO** to cancel.* ***Note:*** If unable to delete (you do not have admin privileges), and Unable to Delete screen appears.



Device identifiers for each Access Point, Station, and Sensor display throughout the AirDefense GUI. Use the User Display Preferences table to determine your display preferences for device identifiers.

> ***Example:*** *Access Points can display throughout the GUI as either a MAC address, an IP address, a Name you select, or as a DNS name.*

Using this table, you can choose an alias over the AirDefense default, which is the cryptic IEEE MAC address for each device type in your network. The preferences you choose in this table determine how you will view data throughout the AirDefense GUI. If you choose not to use MAC addresses, your preference displays any place the MAC address normally displays.



The table below lists the display choices.

Field	Choices
BSS Display Preference	Click on one. Your choice determines how Access Points display in the AirDefense GUI. • **MAC Address:** Displays the IEEE MAC address of the Access Point • **IP Address:** Displays the IP Address of the Access Point (if available) • **Name:** Displays the IP Address of the Access Point (if available) • **DNS:** Displays the DNS name for the Access Point
Station Display Preference	Click on one. Your choice determines how Access Points display in the AirDefense GUI. • **MAC Address:** Displays the IEEE MAC address of the Station • **IP Address:** Displays the IP Address of the Station (if available) • **Name:** Displays the IP Address of the Station (if available). • **DNS:** Displays the DNS name for the Station • **LEAP:** Displays the LEAP (EAP Authentication Mode) name for the Station (See "Create Policy: Configuration" on page 99).
Sensor Display Preference	Click on one. Your choice determines how Access Points display in the AirDefense GUI. • **MAC Address:** Displays the IEEE MAC address of the Sensor • **IP Address:** Displays the IP Address of the Sensor (if available) • **Name:** Displays the IP Address of the Sensor (if available).

Data Export

Use the Data Export feature to do the following:

- Take AirDefense reports, export them into a tab-delimiter file, and then import them into Excel or some other spreadsheet or database system.
- Backup the database.

Report Data Export

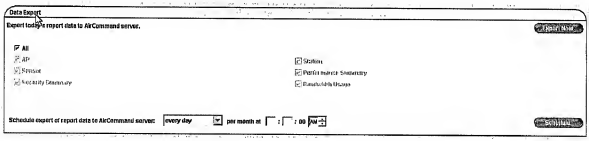
AirDefense generates alarms and records a variety of statistics about your WLAN--device associations, traffic, channel usage, and other important information on the state of AirDefense This data is deleted from AirDefense's database after it is 30 days old.

You can export this data to external files, to run queries against AirDefense. Exporting data is not automated—it requires an administrator. Data is exported in tab-delimited format to a text (.txt) file. At the time of export, AirDefense exports all data of the selected types collected since midnight of the current day.

You can also fully backup and archive the database, or fully restore the database to AirDefense from the backup.

8.3.1 Data Export

Use the data export table to select the categories of data you want included in your report (see the table that follows).



The table below describes the data selections in the Data Export table.

Data Type	Description
All	Selecting All automatically selects all the check boxes below.
AP	Selecting AP will export a report displaying the following information about Access Points detected that day: • **BSS ID:** (The MAC address of each Access Point.) • **SSID:** (The text string identifying the Service Set to which each Access Point belongs.) • **Advertised Channel:** (The channel that each Access Point broadcasts that it is transmitting/receiving on.)

Data Type	Description
Sensor	Selecting "Sensor" will export a report displaying the following information about your Sensors: • **Sensor ID:** (The MAC address of each of your Sensors.) • **Sensor Name:** (The use-configured name of each Sensor.) • **Sensor Group:** (The name of the Group to which the Sensor belongs.) • **Sensor Location:** (The name of the Location to which the Sensor belongs.)
Security Summary	Selecting "Security Summary" will export a report showing the following information: • **Station ID:** (The MAC address of every Station that generated an alarm.) • **Alarm Count:** (The total number of alarms each Station generated during the 24 hour period on that date.)
Station	Selecting "Station" will export a report displaying the following information about all Stations detected that day: • **Station ID:** (The MAC address of each Station.) • **BSS ID:** (The MAC address of the Access Point it associated with.) • **First Seen:** (The timestamp when the Station was first observed that day by the Access Point.) • This column displays the number of Critical alarms that have been generated in the specific 24-hour period. *Note:* While the timestamp at the upper left corner of the browser window reflects the AirDefense clock on your workstation, the time and date values within the application's report tables show the system time of the AirDefense Server. • **Last Seen:** (The timestamp when the Station was last seen by the Access Point.)

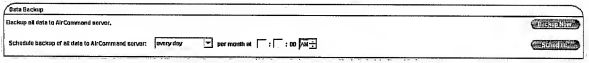
Data Type	Description
Performance Summary	Selecting "Performance Summary" will export a report of WLAN traffic per channel for that date, displaying the following information: • **Advertised Channel:** (The channel on which Access Points are broadcasting that they are transmitting on.) • **Active APs:** (The number of Access Points active on the channel.) • **Active Stations:** (The number of Stations active on the channel.) • **Wireless to Wireless Bytes:** (tbw_intra) (The total number of bytes of data transmitted on that channel within the WLAN.) • **Wireless to Wired Bytes:** (tbw_out) (The total number of bytes of data transmitted from the wireless network to the wired network.) • **Wired to Wireless Bytes:** (tbw_in) (The total number of bytes of data transmitted from the wired network to the wireless network.) • **Wired to Wired Bytes:** (tbw_thru) (The total number of bytes of data originating from the wired network and destined for the wired network.) • **Utilization:** (The total number of bytes transmitted on the channel during the 24-hour period on that date. Note: if the Sensor was scanning multiple channels, this value will only reflect data that was transmitted when the Sensor was listening on that channel.) • **Peak Utilization:** (If the Sensor was scanning multiple channels, the total bytes of data the Sensor heard during its busiest listening period is reported. That is, if the Sensor was scanning channel 6 for ten minutes twice an hour, and of all the ten-minute periods of the day, the most traffic occurred between 12:00—12:10 (one of its listening cycles), the total bytes for that period are reported. Note: if the Sensor is set to monitor one channel continuously, this number will be the sum of "byte" statistics above.)
Bandwidth Usage	Selecting "Bandwidth Usage" will export a report of the Stations' bandwidth usage for date: • **Station ID:** (The MAC address of the Station.) • **Bytes Transmitted:** (tx_bytes) (The total number of bytes of data transmitted that day by that Station.) • **Bytes Received:** (rx_bytes) (The total number of bytes of data received that day by that Station.) • **Advertised Channel:** (The channel over which the data was transmitted or received.)

Steps to Export Data

Step	Action
1	Select one or more data types in the Data Export table.
2	Click **Export Now.**
	Reports are immediately generated and saved on the AirDefense Server.
	A window will pop up, providing you with the path to the exported files. Access the reports from an Xterm window on the AirDefense Server and open the files in a third party application for view and analysis.
	A Export Successful screen appears if the reports successfully export.

8.3.2 Data Backup

Use the table below to schedule a backup of all data to the AirDefense Server.



Steps to Backup Now

Step	Action
1	Click Backup Now to backup data immediately.
	A Scheduling Successful screen appears that indicates your backup was successful.

Steps to Schedule a Backup

Step	Action
1	Schedule a backup using the day and time put-downs.
2	Click Schedule.
	A Scheduling Successful screen appears that indicates your backup was successful.

8.4 Updates & Licenses

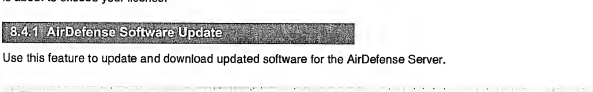
Updates & Licenses

Use the Updates & Licenses table to update the AirDefense software and manage licenses.

The license managing feature provides an automated method for you to monitor Access Points and Sensors license issues. Your administrator is automatically notified when the number of Access Points and Sensors in your network is about to exceed your license.

8.4.1 AirDefense Software Update

Use this feature to update and download updated software for the AirDefense Server.



The table below lists the options and results.

Option	Result
Automatically check for updates	Click this to automate the software upgrade process. Leaving this box unchecked tells AirDefense never to check for updates.
Weekly	Select Weekly for a weekly check for updates.
Monthly	Select Monthly for a monthly check for updates.
Check Now	Press this button to check for updates now. This button overrides the schedules.

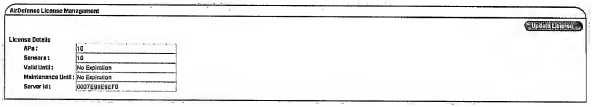
Steps to Upgrade the AirDefense Server Software

Step	Action
1	Click Update Now, or schedule an automatic update.
2	This connects your AirDefense Server to the AirDefense Update AirDefense Server (online). AirDefense checks for updates. If an update is available, the AirDefense Server downloads the update into a directory and informs your administrator that an update is available.
3	If an update is available, connect to AirDefense via SSH, use the ADDadmin utility, and install the upgrade (see "Steps to Log On to a Remote AirDefense Server using the Command Line Interface" on page 9).

8.4.2 AirDefense License Management

Use the AirDefense License Management table to request licenses to authorize more Access Points in your network. The License Details display the parameters of your current license. This field changes when updates take place.

Important: You cannot authorize more Access Points in your network than your current license specifies.



The table below describes the License Details.

License Detail	Meaning
AP	This is the number of Access Points you can use, according to your current license.
Sensors	This is the number of Sensors you can use, according to your current license.
Valid Until	Your license is valid until this date.

License Detail	Meaning
Maintenance Until	This is how long your license will be maintained (some licenses have expiration dates.)
AirDefense Server Id	This is your AirDefense Server ID number.

Steps to Upgrade A License

Step	Action
1	Contact AirDefense, Inc. and request a new license.
2	AirDefense generates a license, and sends you a license file.
3	Once the file is in your possession, Click Upgrade License. *The Select AirDefense License File screen appears.*
4	Double click on the license file. *This updates your License Details.*

8.5 Certificate Manager

Certificate Manager

Use Certificate Manager to create or install a AirDefense Server Security Certificate for your AirDefense Server.

Note: AirDefense recommends that you do this for every AirDefense Server in your network.

Security certificates verify the authenticity of the AirDefense Server (AirDefense generates alarms for untrusted Servers). The AirDefense Server Security Certificate verifies to the administrator that no one has hijacked your administrative session). It provides a TLS-encrypted "tunnel" for the data-flow. AirDefense sends the certificate directly to your browser.

For users whose need for security is paramount, AirDefense, Inc. recommends purchasing and installing a digitally signed Security Certificate from a trusted root Certificate Authority (CA).

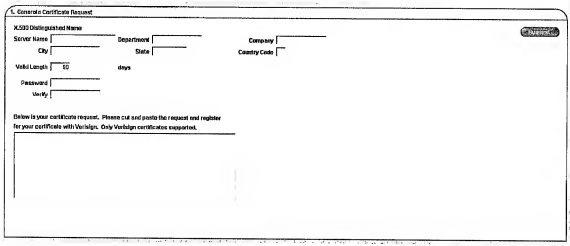
Important: AirDefense currently support VeriSign only.

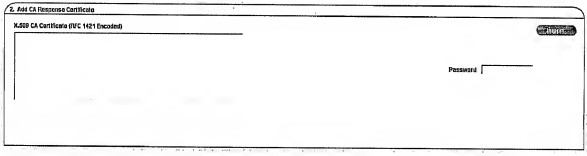
AirDefense Security Certificate

AirDefense ships with a pre-installed Security Certificate on the AirDefense Server. It is a working certificate that provides TLS encryption. However, it has not been digitally signed by a Certificate Authority, and the host name identified in the certificate will not match the actual host name of your AirDefense Server. (Each time you open an administrative session with AirDefense, your browser will report that the Security Certificate is invalid.) You may continue using the default Security Certificate, but your security is minimal.

An intermediate level of security for your administrative sessions may be to generate a Certificate Signing Request (CSR), in which you provide your company and AirDefense Server information, but *do not send the resulting public key to VeriSign* requesting its digital signature. AirDefense will automatically begin using this newly-generated private key/public key pair for a TLS administrative session (see the note below). (The first time you log onto AirDefense, your browser will ask if you want to trust the new Security Certificate *just this once* or *always*. If you select *always*, the warning will never reappear.) However, the session is still vulnerable to being hijacked without detection.

Note: After clicking **Generate**, an alert will prompt you to log on to the Command Line Interface in order to reboot the AirDefense appliance. (See "Services" on page 239 for instructions on rebooting AirDefense from the Command Line Interface.) The new private key/public key pair will not take affect until after AirDefense is rebooted.





8.5.1 Certificate Request

Steps to Generate and Install a Valid Certificate Request

Step	Action
1	Submit a Certificate Signing Request (CSR) to a Certificate Authority.
2	Enter the required data into the input fields (all fields are required). *AirDefense* generates a private key/public key pair, and displays a hash of the public key in the "Certificate Request" field. ***Note:*** If you intend to submit your public key to Verisign for its digital signature, do not click the **Request** button a second time! Doing so will generate a *new* private key/public key pair that will not correspond to the public key Verisign will return to you.
3	Navigate to VeriSign's web site. *You will be prompted to submit information about your organization and the AirDefense Server.*

4 Before completing the online purchase of the certificate, you will be specifically prompted to paste the public key that AirDefense generated. When you copy the key string from AirDefense, you must also include the leading and following "-----BEGIN NEW CERTIFICATE REQUEST-----" and -----END NEW CERTIFICATE REQUEST-----."

Note: Your company may have specific policies regarding what data you must provide with the certificate (e.g., city where the AirDefense Server resides vs. city of corporate headquarters). Consult the correct person in your company, if you have questions about what information to supply.

Fields	Description
AirDefense Server Name	Enter the host or AirDefense Server name you assigned the AirDefense Server.
Department	Enter the Department in which the AirDefense administrator is a member.
Company	Enter the name of your company.
City	Enter the city in which your company is located.
State	Enter the State (full name--*not abbreviated*) in which the company is located.
Country Code	Enter the 2-character country code for the country in which the company is located.
Valid Length	Enter the length of time (in days) you want the Security Certificate to be valid. (Consult with VeriSign for certificate duration.)
Password	Enter a password to be associated with the Security Certificate. (After you receive the Security Certificate from VeriSign, you will be required to provide the same password before installing it on the AirDefense Server.)
Verify	Enter the password a second time to verify its spelling.
Public Key field	Do not enter anything in this field. AirDefense will automatically populate the field with a text string representing the public key of a private key/public key pair after you fill in all other input fields and click **Request.**

5 After VeriSign returns your public key (now containing VeriSign's signature), paste that key string into the **X.509 CA Certificate** field. Enter the password you created when generating the CSR, and click **Import.**

AirDefense installs VeriSign's digitally-signed certificate into the AirDefense Server.

8.6 System

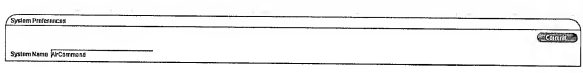
System

Use the System Preferences table to determine a name for the AirDefense Server--*for identification purposes*. The name you choose is the name that will appear at the top of the Directory Tree, in all instances, on the AirDefense GUI.

The name you choose can be no longer than twenty characters.

System Preferences Feature

It is important to use this feature if you have more than one AirDefense Server in your enterprise.



9 Command Line Interface

Use the Command Line Interface to configure the initial settings for the AirDefense Server, and also to configure some settings that are not available within the AirDefense Server graphical user interface (GUI).

Example: *You can change the IP address of the AirDefense Server, reset the AirDefense clock, or set it to sync with an network time AirDefense Server. You can also enhance your security by restricting access to the AirDefense Server to specified IP addresses or subnets.*

9.0.1 In This Chapter

This chapter contains the following topics.

9.1 Access the Command Line Interface

You can access the Command Line Interface from a local location, using a monitor-attached console on the AirDefense Server, or from a remote location, using an SSH (version 2) client for network access.

Note: AirDefense does not allow ftp or telnet sessions. The AirDefense Server will respond to a ping. To disable the ping, see "Network" on page 233.

9.1.1 Launching the Command Line Interface

Steps to Power Up and Log On to a Local AirDefense Server using the Command Line Interface

Step	Action
1	Turn on power to the AirDefense Server. *As the AirDefense Server is booting up, a command-line logon prompt against a black screen will appear on the AirDefense Server console.*
2	At the logon prompt, enter **smxmgr** as your user name and the unique password for your organization.
3	After connecting to the AirDefense Server, enter the following command to launch the Command Line Interface: ADDadmin. *The ADDadmin screen should appear* ***Note:*** The command is case-sensitive.

Steps to Log On to a Remote AirDefense Server using the Command Line Interface

Step	Action
1	Launch your SSH client and connect to the AirDefense Server's IP address.

Note: You must have at least version 2 of a Secure Shell (SSH) client installed on the remote workstation from which you wish to connect to the AirDefense Server.

2 At the logon prompt, enter **smxmgr** as your user name and the unique password for your organization.

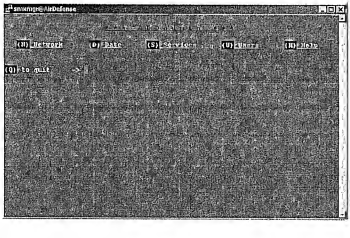
3 After connecting to the AirDefense Server, enter the following command to launch the Command Line Interface:
ADDadmin.

The ADDadmin screen should appear

Note: The command is case-sensitive.

9.2 Command Line Interface Programs

The ADDadmin screen displays in the terminal window. There are five interface program areas at the top of the window.



The table below summarizes the program areas.

Program	This Program...
Network	Has options to change IP address, DNS Servers, hostname, domain name, mail AirDefense Server, ARP, create allow and deny lists, and enable/disable pinging for the AirDefense Server.
Service	Allows you to edit the time and date, set the time zone, and to configure an NTP AirDefense Server.
Date	Enables you to clear the database, reboot, and shut down AirDefense.
Users	Enables you to create, edit, and delete user accounts that allow access to the graphical user interface
Help	Gives you tips on using the application, and detailed help topics.

9.2.1 General Instructions for Using the Interface

The following is a general guide to using the interface.

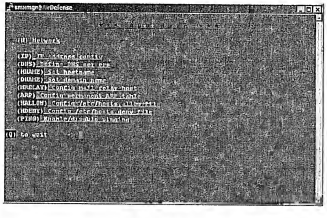
- If you re-size the window so that it is narrow, the program areas display vertically on the left side of the window.
- Typing the letter preceding each program area name at the command prompt takes you to that area.
- Each program area has a variety of commands or functions within it.
- You may type any program command at the opening ADDadmin command prompt—it is not necessary to navigate first to the program page in order to execute a command within it. Whereas mis-typed commands in ADDadmin's secondary pages are forgiven, misspellings at the opening window log you out of the program.
- Each program area contains Commands—text strings used to access a program function—displayed inside a pair of parentheses preceding the command labels. Commands are **not** case sensitive within ADDadmin.
- Typing **q** at the prompt returns you to a parent window, or if at the opening ADDadmin screen, quits the application.
- Once you have make all ADDadmin changes, quit **all the way out** of ADDadmin. AirDefense will automatically reboot, if required.

9.2.2 Network

Step to Open the Network Settings Program Area

Step	Action
1	Type **n** at the command prompt.

This up the Network settings screen.



The table below lists the commands in the Network settings screen.

Command	Description
IP	IP address config Type **ip** to change the IP address, subnet mask, and default gateway for the AirDefense Server you are logged onto. The **IP** configuration screen opens, displaying the current network configuration in bold text. At the prompt, enter a new IP address. After entering a new IP address and pressing **Enter**, you are prompted to enter a new subnet mask. After entering a new subnet mask and pressing **Enter**, you are prompted to enter a new gateway. After entering a new gateway address and pressing **Enter**, your new values are displayed in bold text. If you are logging in remotely using SSH, check these values very carefully for accuracy before typing **yes** or **no** to commit the changes—committing incorrect information will cause you to lose connectivity to the AirDefense Server. AirDefense reboots on exit from the ADDadmin. Typing **yes** or **no** at the prompt to commit the changes returns you to the previous network screen.
DNS	*Define DNS Servers* Type **dns** to add or delete a DNS nameServer. The NameServer screen opens, displaying your current DNS AirDefense Server's IP address in bold text. At the prompt, type either **A** to add a new DNS AirDefense Server, or **D** to delete a AirDefense Server. • **To add an entry:** type **A** at the prompt and enter the IP address at the ensuing prompt. After pressing Enter, the new DNS AirDefense Server is added to the list of nameServers. Note: Multiple DNS Servers have an "order" for processing DNS requests. The first AirDefense Server on the list (identified by the numeral 1) is the first to offer name resolution; the second AirDefense Server on the list (identified by the numeral 2) is the second to process the request if the first is unable to do so. In order to *change* the order preference of multiple Servers, you must delete them all, and re-enter them *in the order you want them to process your DNS requests.* The first AirDefense Server you enter will become number 1—the first to process name resolution. • **To delete an entry: type D** at the prompt and enter at the ensuing prompt the number of the nameServer you want to delete. (If you delete a DNS AirDefense Server that is followed by other Servers, all the ones below with a lower preference will "move up" in priority.) Type **Q** to quit and return to the parent screen; you are prompted to save your changes.

Command	Description
HNAME	Set hostname Type **hname** at the prompt to change the name of the AirDefense Server. The Hostname screen displays your current hostname in bold text. At the prompt, enter a new name for the AirDefense Server you are currently connected to. After pressing **Enter**, you are prompted to commit the change. (Type **yes** or **no**.) *Note:* AirDefense reboots on exit from the ADDadmin. *Note:* Whenever you change the name of the AirDefense Server, its name must also be modified in all devices that refer to it (e.g., DNS Servers).
DNAME	Set domain name Type **dname** at the prompt to change the domain to which the AirDefense Server belongs. The Domain name screen displays your current domain name in bold text. At the prompt, enter a new name for the domain to which you belong. After pressing **Enter**, you are prompted to commit the change. (Type **yes** or **no**.) *Note:* AirDefense reboots on exit from the ADDadmin. *Note:* Whenever you change the domain name of the AirDefense Server, its domain name must also be modified in all devices that refer to it (e.g., DNS Servers).
MRELAY	Config AirDefense Server to "point" to a mail relay host You must configure your mail AirDefense Server to allow the AirDefense Server to relay email messages through it, or at least to direct its mail to another mail AirDefense Server that will relay email. In addition, you must define at least one DNS AirDefense Server for this function to operate correctly. Type **mrelay** at the prompt to configure AirDefense to send alarms by email. The Mail relay host screen appears. Type **A** to add an entry, or **D** to delete an entry. • **To add an entry:** type **A** at the prompt and enter the IP address or fully qualified hostname (e.g., myhostname.mydomainname.com) of a mail AirDefense Server to process email alarm messages. After pressing **Enter**, the mail AirDefense Server is added to the list of servers. • **To delete an entry:** type **D** at the prompt and enter at the ensuing prompt the number of the mail AirDefense Server you want to delete. After typing **Q** to return to the parent screen, you are prompted to save your changes. Type **yes** or **no**.

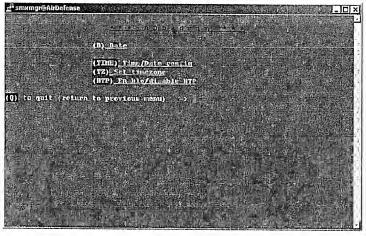
Command	Description
ARP	Config permanent ARP table Type **arp** at the prompt to create a permanent ARP table. The ARP screen displays your current ARP records in bold text. In order to protect connections between this AirDefense Server and remote administrators from being hijacked by man-in-the-middle ARP "blasts" (that redirect traffic for this IP address to an alternate MAC address), create permanent ARP records for your gateway and other important machines. • **To add an entry:** type **A** at the prompt and enter the hardware (MAC) address of a router or machine. Next enter the IP address associated with the MAC address. After pressing **Enter,** the machine is added to the ARP table. Now, when opening a connection to that machine, it will *first* look in its own ARP table to discover how to connect to it, instead of relying on an ARP broadcast. • **To delete an entry:** type **D** at the prompt and enter at the ensuing prompt the number of the record in the ARP table you want to delete. After typing **Q** to return to the parent screen, you are prompted to save your changes. Type **yes** or **no.**
PING	Type **ping** at the prompt to change the ping setting for the AirDefense Server. Ping enabled (default) makes it possible for you to ping the AirDefense Server from a remote location. A status line at the top of the screen indicates the current status. • **E:** type **E** at the prompt, then **Enter** to enable pinging (default). The status line reads Pinging currently enabled. • **D:** type **D** at the prompt, then **Enter** to disable pinging. The status line reads Pinging currently not enabled.

Command	Description
HALLOW	Configure/etc/hosts.allow file Type **hallow** at the prompt to specify which systems are allowed to connect to the AirDefense Server. The Allow list screen displays your current list of allowed workstations and laptops in bold text. You may specify which systems are allowed to connect to a AirDefense Server. Only those whose IP address, subnet, fully qualified hostname, or domain name match an entry in this list are allowed to connect to a AirDefense Server to run ADDadmin. • **To add an entry:** type **A** at the prompt and enter either a single host IP address (123.456.789.963), class A, B, or C subnet (123., 123.456., 123.456.789.—note the trailing "." in the subnets), fully qualified hostname (myhostname.mydomainname.com), or domain name at the ensuing prompt. Anyone within a specified subnet, or from a specified host or domain may connect to a AirDefense Server. Repeat as desired. • **To delete an entry:** type **D** at the prompt and enter at the ensuing prompt the number of the record in the allow table you want to delete. After typing **Q** to return to the parent screen, you are prompted to save your changes. Type **yes** or **no.**
HDENY	Config /etc/host.deny file Type **hdeny** at the prompt to specifically identify systems that may not connect to the AirDefense Server. The Deny list screen displays your current list of denied systems in bold text. You may specify which systems are *not* allowed to connect to a AirDefense Server. Anyone whose IP address, subnet, fully qualified hostname, or domain name matches an entry in this list are **not** allowed to connect to a AirDefense Server to run ADDadmin. *Note:* HALLOW takes precedence over HDENY. For example, if 123.456.789.963 is on the allow list, yet the subnet 123.456.789. is on the deny list, the individual system above is allowed to connect to the AirDefense Server. • To add **an entry:** type **A** at the prompt and enter either a single host IP address (123.456.789.963), class A, B, or C subnet (123., 123.456., 123.456.789—note the trailing "." in the subnets), fully qualified hostname (myhostname.mydomainname.com), or domain name at the ensuing prompt. Anyone within a specified subnet, or from a specified host or domain is not allowed to connect to the AirDefense Server. Repeat as desired. • **To delete an entry:** type **D** at the prompt and enter at the ensuing prompt the number of the record in the "allow" table you want to delete. After typing **Q** to return to the parent screen, you are prompted to save your changes. Type **yes** or **no.** *Note:* Do not unwittingly lock yourself out of the AirDefense Server by creating a deny policy that affects your WLAN. Ensure that you create an allow policies for yourself.

9.2.3 Date

Step to Open the Date Program Area

Step	Action
1	Type d at the command prompt. *This brings up the Date settings screen.*



The table below lists the commands available in the Date settings screen.

Command	Description
TIME	Time/Date config Type time to change the AirDefense Server's operating time and date. The current date and time is displayed in bold text. You are prompted to enter a date in MMDDYYYY format. (Do not use colon, forward slash, or other delimiters.) After pressing **Enter**, you are prompted to enter a time in 24-hour HHMM or HHMMSS format. After pressing **Enter**, you are prompted to save your changes (type **yes** or **no**). AirDefense reboots on exit from the ADDadmin.

Command	Description
TZ	Set time zone Type **tz** to edit the time zone in which the AirDefense Server resides. The Time zone screen displays a list of global, continental regions. Enter the corresponding number (to the left of your region name) and press **Enter**. In the next screen, enter the abbreviation of your nationality (to the left of the nation) in which the AirDefense Server resides, and press **Enter**. In the next screen, enter the number of the region within your nationality in which the AirDefense Server resides, and press **Enter**. You are prompted to save your changes (type yes or no). Typing yes or no reboots *and clears* the database on exit from the ADDadmin.
NTP	Enable/disable NTP Type **ntp** to enable automatic "time synching" with a network time AirDefense Server, and to specify the time AirDefense Server. The NTP screen displays your current status in bold text—whether or not you are currently set to use NTP. Type **E** to enable NTP. You are prompted to enter the IP address or fully qualified hostname (hostname.domainname.com) of a network time AirDefense Server. To save the time AirDefense Server settings, type **Q** to quit this program area—you are prompted to save your settings. Entering an invalid time AirDefense Server generates an error and logs you out of the ADDadmin. Type **D** to disable NTP. No additional input is required—NTP is immediately disabled.

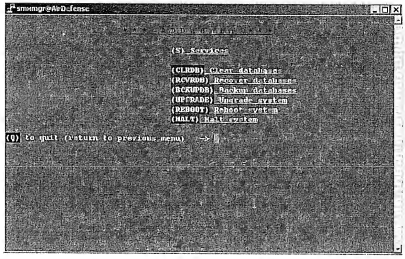
Note: If you change the AirDefense time because, for example, you move the AirDefense Server's location from the east to west coast of the United States, you must also locate a *new* network time AirDefense Server in the same time zone.

9.2.4 Services

The Services program area allows you do clear the AirDefense Server database, to reboot the AirDefense Server GUI, or to completely halt AirDefense Server operation.

Step to Open the Services Program Area

Step	Action
1	Type s at the command prompt. *The Services settings screen displays.*



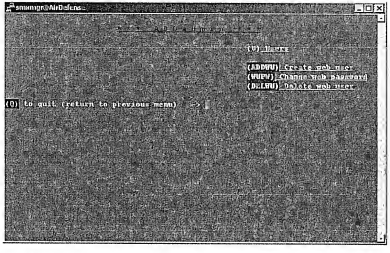
The table below lists the commands available in the Services settings screen.

Command	Description
CLRDB	Clear database Type **clrdb** to delete and rebuild AirDefense's database. You are prompted to confirm the command by typing **yes** or **no**. **No** returns you to the Services page leaving the database untouched. **Yes** deletes the database and returns you to the Services page. This commands deletes and rebuilds the AirDefense database. It deletes network traffic statistics and policies settings. Use this command, for example, when you move AirDefense to a new network and want to start fresh with new policies and data.
REBOOT	Reboot AirDefense Type **reboot** to gracefully restart the AirDefense Server. The AirDefense Server automatically shuts down and restarts.
HALT	Halt AirDefense Type **halt** to gracefully shutdown AirDefense. AirDefense immediately runs its shutdown routine.

9.2.5 Users

Step to Open the User's Program Area

Step	Action
1	Type u at the command prompt. *The User's settings screen displays.*



The table below lists the commands available in the User's settings screen.

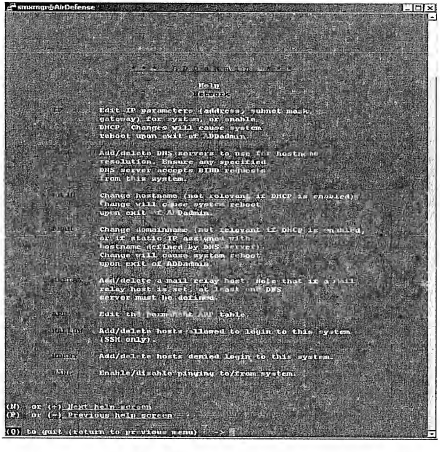
Command	Description
ADDWU	Use this command to create a new web user. Once you enter the command, prompts appear that allow you to do the following: • Add an entry — Type the name of the new user to add — Enter new password — Enter new password again — Save the web entries as shown (yes/no) • Delete an Entry — Type the name of the user to delete — Save the web entries as shown (yes/no).

Command	Description
WUPW	Use this command to change password for web user. Once you enter the command, prompts appear that allow you to do the following: • Add an entry — Type the name of the user for the password change — Enter the current password for the user — Enter the new password — Enter the new password again — Change the password for this user (yes/no) • Delete an Entry
DELWU	Use this command to delete a web user. Once you enter the command, prompts appear that allow you to do the following: • Add an entry — Type the name of the new user to add — Enter new password — Enter new password again — Save the web entries as shown (yes/no) • Delete an Entry — Type the name of the user to delete — Delete this user (yes/no)

9.2.6 Help

Step to Open the Help Program Area

Step	Action
1	Type h at the command prompt. *This brings up the Help screen.*



The table below lists the commands available in the Help screen.

Command	Description
N or +	Prompts at the bottom of the Help window show that typing **N** (Next) or the Plus sign (**+**) advances the Help window. The Help window begins at the first menu item: Network. Each time you enter **n** or **+**, the Help window advances to the next topic. Beginning at the Network Help window, successively entering **+** or **n** yields the following navigation path: **+** <Enter> ➲ Date; **+** <Enter> ➲ Services; **+** <Enter> ➲Users.
P or -	Prompts at the bottom of the Help window show that typing **P** (Previous) or the Minus sign (-) reverses the Help window. If at Users, the last Help window, successively entering "-" or "p" yields the following navigation path: **-** <Enter> ➲ **Services**; **-** <Enter> ➲ **Date**; **-** <Enter> ➲ **Network**.

Appendix A: Alarms

AirDefense automatically generates alarms whenever certain events or conditions occur within your wireless network. The majority of alarms are specific to the Sensor. System Alarms are usually specific to the AirDefense Server.

You can view alarms AirDefense's Alarm Manager. In addition, alarms can be delivered to the administrator by email or SNMP. When you select an individual alarm in the Alarm Manager's table of alarms, details are displayed at the bottom of the page. You can identify each alarm by classification and type. There are five classifications of alarms:

- **Attack:** WLAN traffic indicative of an attack against the network.
- **Policy:** WLAN traffic that violates established WLAN policies.
- **Performance:** WLAN traffic that exceeds user-defined performance thresholds.
- **Event:** Unexpected changes in the way Access Points operate.
- **System:** AirDefense components or failing to perform as designed.

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Attack	DOS De-Auth	**Denial of Service De-authentication** Occurs when an attacker is *spoofing* the MAC address of an Access Point and is either telling a specific host or all hosts to de-authenticate.	Critical
	DOS Disassoc	**Denial of Service Disassociation** Occurs when an attacker is spoofing the MAC address of an Access Point and is either telling a specific host or all hosts to disassociate.	Critical
	DOS Excessive MACs	**Denial of Service Excessive MACs** Occurs when an excessive number of MAC addresses have appeared in the wireless network. This generally means an attacker is spoofing these addresses to flood the network and create a DOS by sheer volume.	Critical
	Identity Theft: Out of Sequence	**Identity Theft: Out of Sequence** AirDefense's Analysis Engine keeps track of frame sequence numbers as sessions are started between an Access Point and a Station. If these numbers diverge too greatly it is possible that a third party may be stealing the identity of the Station and starting their own session.	Critical

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Attack Continued	Identity Theft: Vendor Mis-match	**Identity Theft: Vendor Mismatch** Occurs when the vendor identity determined by the MAC address is not the same as the vendor's usual signature.	Critical
	Network Scan Net Stumbler Detection	**Network Scan** Occurs when the user that someone using a tool like NetStumbler is currently scanning their wireless network.	Critical
	Network Scan AirMagnet	**Network Scan AirMagnet** Occurs when the tool AirMagnet has started. While the tool is running, it is completely passive, which is why we can only see it start.	Critical
	Network Scan Wellenreiter	**Network Scan Wellenreiter** Occurs when the tool Wellenreiter has started. Wellenreiter is an open source tool that performs discovery, penetration, and auditing of 802.11b networks.	Critical
Policy	Unauth Station	**Unauthorized Station** Occurs when a Station is associating with an Access Point for which it is not authorized (on the Access Point's valid Station list). Alarms do not generate for Stations associated with unauthorized Access Points.	Critical
	Unauth AP	**Unauthorized AP** Occurs when an Access Point appears in the network and the administrator has not indicated it is authorized to be there.	Critical
	AP Policy: WEP	**AP Policy: WEP** Occurs when the administrator has specified a WEP mode policy for an Access Point and the Access Point is not following it.	Critical
	AP Policy: SSID in Beacon	**AP Policy: SSID in Beacon** Occurs when the SSID is being sent in the Access Point's beacon, even though the administrator has specified that the SSID is not to be sent in the Access Point beacon.	Critical

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Policy Continued	AP Policy: Rate Violation	**AP Policy: Rate** Occurs when the Access Point is advertising data rates not specified in the Access Point policy screens.	Critical
	AP Policy: Auth Mode Violation	**AP Policy: Auth Mode Violation** Occurs when the administrator has specified an authentication mode policy and the Access Point is not following the specified policy.	Critical
	AP Policy: Channel	**AP Policy: Channel** Occurs when the administrator has specified the channel the Access Point should use, but the Access Point is transmitting over a channel other than the one specified.	Critical
	Policy Roaming	**Policy Roaming** Occurs when a Station that is authorized on at least one authorized Access Point associates to another authorized Access Point, but for which the Station is not authorized.	Critical
	Policy Vendor	**Policy Vendor** Occurs when a Station associates to an authorized Access Point, but the vendor of the wireless card does not match the Vendor Policy that is defined for that Access Point.	Critical
	Channel Policy: Time of Day Violation	**Channel Policy: Time of Day** Occurs when any Station transmits on a specific channel at a time that is outside the administrator-indicated valid Time of Day (policy set per Sensor).	Critical
	Channel Policy: Ad-Hoc Network Detected	**Channel Policy: Ad-Hoc Network Detected** Occurs if a Station is seen sending or receiving any ad hoc frames when the Sensor's policy is set to not allow ad hoc.	Critical
Performance	Assoc Max Exceeded for AP	**Associations Max Exceeded in BSS** Occurs when the total number of associations allowed on in a BSS in a one minute interval has been exceeded.	Major

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Performance Continued	Fragmented Frames Exceeded for AP	**# of Fragmented Frames Detected in a BSS Threshold** Occurs when the number of fragmented frames allowed in a particular BSS, in a one-minute period, has been exceeded.	Major
	Decrypt Err in BSS	**# Decryption Errors in BSS Threshold** Occurs when the total number of decryption errors allowed in a particular BSS, in a one-minute period, has been exceeded.	Minor
	Station Assoc in BSS Exceeded	**# of Associated Stations in BSS Threshold** Occurs when the total number of Stations allowed to be associated in the BSS corresponding to the Access Point, in a one-minute period, has been exceeded.	Minor
	TBW Into BSS Exceeded	**Total BW In per BSS Threshold** Occurs when the total number of bytes allowed to enter the network of a specific Access Point from the wired network in one minute has been exceeded.	Minor
	TBW Out of BSS Exceeded	**Total BW Out per BSS Threshold** Occurs when the total number of bytes allowed to leave the network of a specific Access Point to the wired network in one minute has been exceeded.	Minor
	TBW Intra BSS Exceeded	**Total BW within BSS Threshold** Occurs when the total number of bytes allowed to be sent from one wireless Station to another wireless Station within the BSS in one minute has been exceeded.	Minor
	TBW Thru BSS Exceeded	**Total BW thru BSS Threshold** Occurs when the total number of bytes allowed to move thru an Access Point's network, whose origination and destination are wired portions of the network, in one minute has been exceeded.	Minor
	Data Frames in BSS Exceeded	**Data Frames in BSS Threshold** Occurs when the total number of data frames sent in a specific BSS in one minute has been exceeded.	Major

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Performance Continued	MGT Frames in BSS Exceeded	**Management Frames in BSS Threshold** Occurs when the total number of management frames sent in a specific BSS in one minute has been exceeded.	Major
	Control Frames in BSS Exceeded	**Control Frames in BSS Threshold** Occurs when the total number of control frames sent in a specific BSS in one minute has been exceeded.	Major
	Station Assoc to AP Exceeded	**# Associations for Station Threshold** Occurs when the total number of associations a Station is allowed to make to one Access Point in one minute has been exceeded.	Major
	Station Frag Frames Exceeded	**# Fragmented Frames for Station Threshold** Occurs when the total number of fragmented frames a Station is allowed to receive in one minute has been exceeded.	Minor
	Station Decrypt Error Exceeded	**# Decryption Errors for Station Threshold** Occurs when the total number of decryption errors a Station is allowed to received in one minute has been exceeded.	Major
	TBW RX for Station Exceeded	**Total Bytes Received for Station Threshold** Occurs when the total bytes a Station is allowed to receive (whether Access Point or Station) in one minute has been exceeded.	Minor
	TBW TX for Station Exceeded	**Total Bytes Transmitted for Station Threshold** Occurs when the total bytes a Station is allowed to transmit (whether Access Point or Station) in one minute has been exceeded.	Minor
	Data Frames RX for Station Exceeded	**Data Frames RX for Station Threshold** Occurs when the total number of data frames a Station is allowed to receive in one minute has been exceeded.	Major

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Performance Continued	Data Frames TX for Station Exceeded	**Data Frames TX for Station Threshold** Occurs when the total number of data frames a Station is allowed to transmit in one minute has been exceeded.	Major
	Mgt Frames RX for Station Exceeded	**Management Frames RX for Station Threshold** Occurs when the total number of management frames a Station is allowed to receive in one minute has been exceeded.	Major
	Mgt Frames TX for Station Exceeded	**Management Frames TX for Station Threshold** Occurs when the total number of management frames a Station is allowed to transmit in one minute has been exceeded.	Major
	Control Frames RX for Station Exceeded	**Control Frames RX for Station Threshold** Occurs when the total number of control frames a Station is allowed to receive in one minute has been exceeded.	Major
	Control Frames TX for Station Exceeded	**Control Frames TX for Station Threshold** Occurs when the total number of control frames a Station is allowed to transmit in one minute has been exceeded..	Major
	CRC Errors Exceeded	**CRC Errors for Sensor Threshold** Occurs when the total number of CRC Errors any given channel should see on a given Sensor in a one minute interval has been exceeded.	Major

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
Event	AP Mode Change: cf Change	**AP Mode Change: cf Change** Occurs when the polling of an Access Point changes (the mechanism by which APs know when it's OK to transmit without colliding with another Access Point).	Minor
	AP Mode Change: ESS ID Change	**AP Mode Change: ESS ID Change** Occurs when the SSID of an Access Point changes.	Critical
	On Watch List	**Watch List** Occurs when a Station that has been placed on the Watch List is active in the WLAN	Critical
	Network Scan XP Protection	**Network Scan: XP Protection** Occurs when a user on Windows XP is using tools provided by XP to scan the WLAN.	Critical
System	Sensor PCM-CIA Failure	**Sensor PCMCIA Failure** Occurs when if the PCMCIA card in the Sensor appears to be malfunctioning. If the wireless card is missing it will generate this alarm every minute.	Critical
	Sensor IO Error	***Sensor IO Error*** Occurs when there is a general fault of the Sensor. This alarm may require the user to power cycle the Sensor.	Critical
	Sensor Auth Failure	**Sensor Auth Failure** Occurs when a Sensor connects to the AirDefense Server, but fails to authenticate.	Critical
	Sensor Heart Beat TO	**Sensor Heart Beat TO** Occurs when a Sensor is connected, it will communicate with the AirDefense Server continuously either by sending data or by sending a heartbeat. If the AirDefense Server fails to receive a heartbeat but is still connected this alarm will occur.	Critical
	Sensor Msg Queue Full	**Sensor Msg Queue Full** AirDefense queues messages from Sensors for processing. Occurs when this queue grows too large.	Critical

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
System Continued	Sensor MAX Reached	**Sensor MAX Reached** The AirDefense Server will only allow a set number of Sensors to attach to any one AirDefense Server. Occurs when this number is exceeded.	Critical
	Sensor Auth Failure	**Sensor Auth Failure** Occurs when a Sensor connects to the AirDefense Server, but fails to authenticate.	Critical
	Sensor Heart Beat TO	**Sensor Heart Beat TO** Occurs when a Sensor is connected, it will communicate with the AirDefense Server continuously either by sending data or by sending a heartbeat. If the AirDefense Server fails to receive a heartbeat but is still connected this alarm will occur.	Critical
	Sensor Msg Queue Full	**Sensor Msg Queue Full** AirDefense queues messages from Sensors for processing. Occurs when this queue grows too large.	Critical
	Sensor MAX Reached	**Sensor MAX Reached** The AirDefense Server will only allow a set number of Sensors to attach to any one AirDefense Server. Occurs when this number is exceeded.	Critical
	Sensor Comm. Out of Spec	**Sensor Comm. Out of Spec** Occurs when a Sensor that is communicating with the AirDefense Server sends something that is out of the protocol specification.	Critical
	Sensor Conn. Queue Full	**Sensor Conn. Queue Full** Occurs if there are a number of Sensors that have connected but have not attempted to authenticate (in this case there's a good chance these are not really Sensors).	Critical
	Sensor Hardware Failure	**Sensor Hardware Failure** Occurs when a Sensor hardware or firmware failure causes the Sensor to loose connection with the AirDefense Server.	Critical

Alarm Classification	Alarm Type	Alarm Name & Description	Alarm Priority
System Continued	Sensor Failed Login	**Sensor Failed Login** Occurs when the login passwords are not recognized by AirDefense.	Critical
	Sensor Offline	**Sensor Offline** Occurs when the Sensor goes offline from the Server.	Critical

Appendix B: File Import Formats

This Appendix contains the following:

- File Format for Importing Access Points
- File Format for importing Stations

File Format for Importing Access Points

The file for importing access points should contain rows of data, one row for each Access Point being imported into your AirDefense WLAN. Each row is separated by a carriage return or new line character. Each row should be a comma-separated list of field values as defined below.

```
mac address, alias, ip address, dns name, description, authorize
```

Field Name	Valid Values
mac address	Valid mac address
alias	Text string or null if not defined
ip Address	Valid ip address or null if not defined
dns name	Text string or null if not defined
description	Text string or null if not defined
authorize	yes or no
bridge	yes or no

Examples

```
aa:aa:aa:aa:aa:aa, My Access Point, 172.16.0.232, machine@xyz.com, this is my access
point, yes, yes

bb:bb:bb:bb:bb:bb, AP B, 145.16.0.232, box2@xyz.com, null, no, no
```

The file for importing stations should contain rows of data, one row for each station being imported into your AirDefense WLAN. Each row is separated by a carriage return or new line character. Each row should be a comma-separated list of field values as defined below.

```
mac address, alias, ip address, dns name, description, authorize
```

Field Name	Valid Values
mac address	Valid mac address
alias	Text string or null if not defined
ip Address	Valid ip address or null if not defined
LEAP Username	Text string or null if not defined
dns name	Text string or null if not defined
description	Text string or null if not defined
authorize	yes, no or null If yes or no is selected, the next field (aplist) should be defined and this station will be either authorized (yes value) or unauthorized(no value) for every access point in aplist
aplist	all (for all access points), comma-separated list of access point mac addresses

Examples

```
cc:cc:cc:cc:cc:cc, Station C, LEAP Username C, 172.16.0.232, machine1@xyz.com, this is
my access point, yes, all
dd:dd:dd:dd:dd:dd, Station D, LEAP Username D, 145.16.0.232, machine2@xyz.com, null,
no, aa:aa:aa:aa:aa:aa, bb:bb:bb:bb:bb:bb
ee:ee:ee:ee:ee:ee, Station E, null, 123.16.0.232, machine3@xyz.com, this is station e,
null
ef:ef:ef:ef:ef:ef, Station EF, null, 123.16.0.232, machine3@xyz.com, this is station
fe, yes, aa:aa:aa:aa:aa:aa
ef:ef:ef:ef:ef:ef, Station EF, null, 123.16.0.232, machine3@xyz.com, this is station
fe, no, bb:bb:bb:bb:bb:bb

Station C will be entered into the system, authorized on all access points.
Station D will be entered into the system, unauthorized on access points
aa:aa:aa:aa:aa:aa, bb:bb:bb:bb:bb:bb.
Station E will be entered into the system with configuration information only.
Station EF will be entered into the system, authorized on access point
aa:aa:aa:aa:aa:aa, unauthorized on bb:bb:bb:bb:bb:bb.
```

Appendix C: Upgrading Sensor Firmware

This Appendix contains the following:

- How to Upgrade the Sensor Firmware

How to Upgrade the Sensor Firmware

AirDefense, Inc. makes upgrades available for the Sensor firmware.

Steps to Upgrade the Sensor Firmware

Follow the steps below to upgrade the Sensor firmware

1. Check your current Sensor firmware version.

   To do this, using your browser, log on to a Sensor from your laptop or workstation.

   Enter the IP address for your Sensor in your browser window.

   - **Use http://** and your Sensor's IP address if you have software version 2.0 or 2.1.
   - **Use https:// or http,** and your Sensor's IP address if you have software version 2.5.

   You are prompted for a user name and password:

   User Name: ***admin*** *(default)*
   Password: ***airsensor*** *(default)*

   The Sensor Web Configuration screen appears.

2. In this screen, check the firmware version in the **Identity: Software Version** field.
3. Compare this against the currently available firmware version. You can find this by going to: http://www.airdefense.net/support/firmware/current/

   If you choose to upgrade, download the current firmware ***locally****. Use your browser to select the firmware file and download.*

   For example, if your current firmware version is 2.0.5.8, and the file in the current directory is "s2106.img.signed" (2.1.0.6), this indicates that a more current firmware version is available.

4. Log on to your Sensor (see step 1).
5. In Update at the bottom of the Sensor Web Configuration screen, Click **Browse** to navigate to the locally saved firmware file and select the file.
6. Click **Upload File.**

   The Sensor firmware automatically upgrades. This process will take from one to two minutes, after which a status screen appears indicating success ("Successfully Programmed"), or failure ("Bad Flash Image").

   If you receive a success indicator, you are finished.
   If you receive a failure indicator, go to step 3.

   Note: During the upload process, the Sensor goes offline. It returns to an online state on completion of the upload.

7. Reboot the Sensor and repeat the firmware upload.

Note: A failure indicator takes place if: 1) An incorrect file was uploaded, or 2) the upgrade was interrupted on the Sensor end, for example, by a power outage. Both require that you repeat the Upload. During the upgrade process, the Sensor receives the new firmware file, checks the data, and burns the data into its flash memory. If a power interruption takes place during this process, the Sensor will either reboot itself, or will have to be remotely rebooted. In this case, the Sensor reverts back to its factory-installed firmware version.

Appendix D: Glossary

This Appendix contains the following:

- Terms and definitions of wireless terms

Terms and Definitions

Wireless networking has a few terms and abbreviations that represent key technologies.You will find the following terms throughout this guide.

Term	Definition
Access Point (AP)	An Access Point is a small device (usually smaller than a laptop or CD carrying case) that transmits and receives network traffic over fourteen radio channels, as specified by the 802.11 protocol (only 11 channels are authorized for wireless network use within the U.S.). An Access Point physically connects to your network via a standard Ethernet cable connection, and acts as a hub for nearby laptops and workstations that are configured with wireless network adapters. Access Points may use a variety of antenna configurations, with each antenna offering specific functionality, such as 360 degree accessibility, line-of-sight accessibility, high gain (strong signal strength), etc.
Ad Hoc Networking	Ad hoc networking is when two or more wireless devices associate with each other without the use of an intermediary Access Point. The software that controls the functionality of wireless network adapters typically provides the ability, configured manually, to accomplish this. The software creates a session ID—much like the MAC address of an Access Point—which the devices use to communicate with each other.
Ad Hoc Station	An ad hoc station is a User Station that is connected to one or more other User Stations without using an Access Point. Ad hoc networking is a function of most standard 802.11 network client cards. User Stations that are connected in this manner do not need a wireless infrastructure, and therefore represent a security threat, especially when one or more User Stations in the ad hoc network also connect to a wired network.
ARP	Address Resolution Protocol. ARP is a TCP/IP protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. ARP returns the layer 2 address for a layer 3 address. ARP requests are broadcast onto the network, requiring every station in the subnet to process the request.

Term	Definition
Basic Service Set (BSS)	Basic Service Set (BSS) is the term that describes the *footprint* of a single Access Point and all User Stations (laptops and workstations) associated with it. The BSS is a footprint in that only User Stations within a certain radius of the Access Point will be able to transmit to, and receive data from the Access Point. Further away, the radio signals will be too weak for successful data transmission. Each BSS has an ID (or identifier) This is the MAC address of the wireless network adapter on that Access Point.
Bridge	Ordinarily, each Access Point is physically connected to the wired network via standard Ethernet cable. There may be instances in which the Extended Service Set is so large (in terms of physical space) that the wired network is several Access Points away. In this case, two or more Access Points serve as bridges to the wired network. Unlike regular Access Points, bridges do not have an Ethernet connection to the physical network. They are configured to transmit data they receive to a specific Access Point—either another bridge or to a wired AP.
Device	A Sensor, Access Point, or User Station in an AirDefense WLAN. How each is represented in the AirDefense GUI is influenced by user preference settings.
Domain Name	This is the name that identifies a web site. For example, "apple.com" is the domain name of Apple Computer's web site. A single web server may have more than one domain name, but a single domain name points to only one machine. For example, www.apple.com, support.apple.com, and store.apple.com could be served on one to three machines. It is also possible, and quite common, for a domain name to be registered, but not be connected to an actual machine. The reason for this is usually so that a company or group can have e-mail addresses at a certain domain without having to maintain a web site. In these cases, there still must be a machine to handle the mail of the listed domain name.
DNS	Domain Name System. This is the name of a web address, as opposed to its actual IP address. Web sites are actually located by their IP addresses. So, when you type in http://www.airdefense.net, the computer doesn't immediately know that it should look for the AirDefense, Inc. web site. Instead, it sends a request to the nearest DNS server, which matches an IP address to the domain name and then connects you to the server with that IP number.
Extended Service Set / Service Set ID (ESS/SSID)	Logical groupings of one or more Access Points (or BSSs) are called an Extended Service Set, and the names that identify them are called Service Set IDs. Each Extended Service Set represents a wireless extension of the wired network. There is no requirement that the Access Points in an Extended Service Set be in physical proximity to each other, or for example, are all on the same floor of a building. The grouping of Access Points into a wireless network is at the discretion of the network administrator. When a User Station wishes to use the services of an Access Point, it must broadcast a probe request announcing the Extended Service Set it wishes to become a part of. The nearest Access Point in that ESS authenticates it and allows network connectivity through it.
Groups	Groups denote clusters of individual Sensors, with each Sensor monitoring the activity of one or more Access Points. Beneath Groups are the Sensors, themselves, represented by an icon of a single Sensor.

Term	Definition
Host Name	This is the name of a computer that acts as a server for other computers on the network. It can be a web server, an email server, an FTP server, etc. For instance, a web host is what provides the content of web pages to the computers that access it.
Locations	Locations are the top-level descriptors in the AirDefense Graphical User Interface program tree. Depending on the size of your wireless network, Locations (represented by a globe icon) can denote a cluster of buildings, or even a city, containing any number of offices. Below Locations on the hierarchy are Groups (represented by an icon of multiply-connected Sensors).
MAC Address	The MAC (media access control) address is the network address used by the 802.11 protocol to identify the physical address of a device. Each 802.11 User Station and Access Point ship with a unique MAC address.
Ping	The main purpose of a ping is to test a system on the Internet to see if it is working. Pinging a server can also test and record the response time of servers and other computers connected to the Internet. This is helpful in finding Internet bottlenecks, so that data transfer paths can be re-routed the most efficient way. Also, a good way to make sure you do not get disconnected from your ISP for being idle is to send a ping every 5 minutes or so. There are a number of shareware Ping programs that will do this for you.
User Station	A User Station is any network device that associates with an Access Point. (To associate with an Access Point is to be authorized as a valid user of the Access Point's services, though some Access Points may be configured to not require authorization.)
WLAN	The wireless Local Area Network (WLAN) refers to that portion of your enterprise network whose medium for data transfer is the radio airwave using the fourteen channels specified by the 802.11 protocol (only eleven channels are authorized for WLAN use within the U.S.).

A

B

T

User Guide r3.0

AirDefense User Guide
Issue 1.02, AD-UG-1.02
Release 3.0

11475 Great Oaks Way
Suite 200
Alpharetta, Georgia 30022
770-663-8115
www.airdefense.net
info@airdefense.com

AirDefense